Comparative Review: SharePoint Backup p. 53

Windows® IT Pro

NOVEMBER 2008 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

SBS 2008 AND EBS 2008 REVEALED!

- Microsoft's Intentions p. 27
- The View from the Trenches p. 29

Group Policy:
Secure Windows Desktops p. 33

Windows Vista:
To Deploy or Not to Deploy p. 38

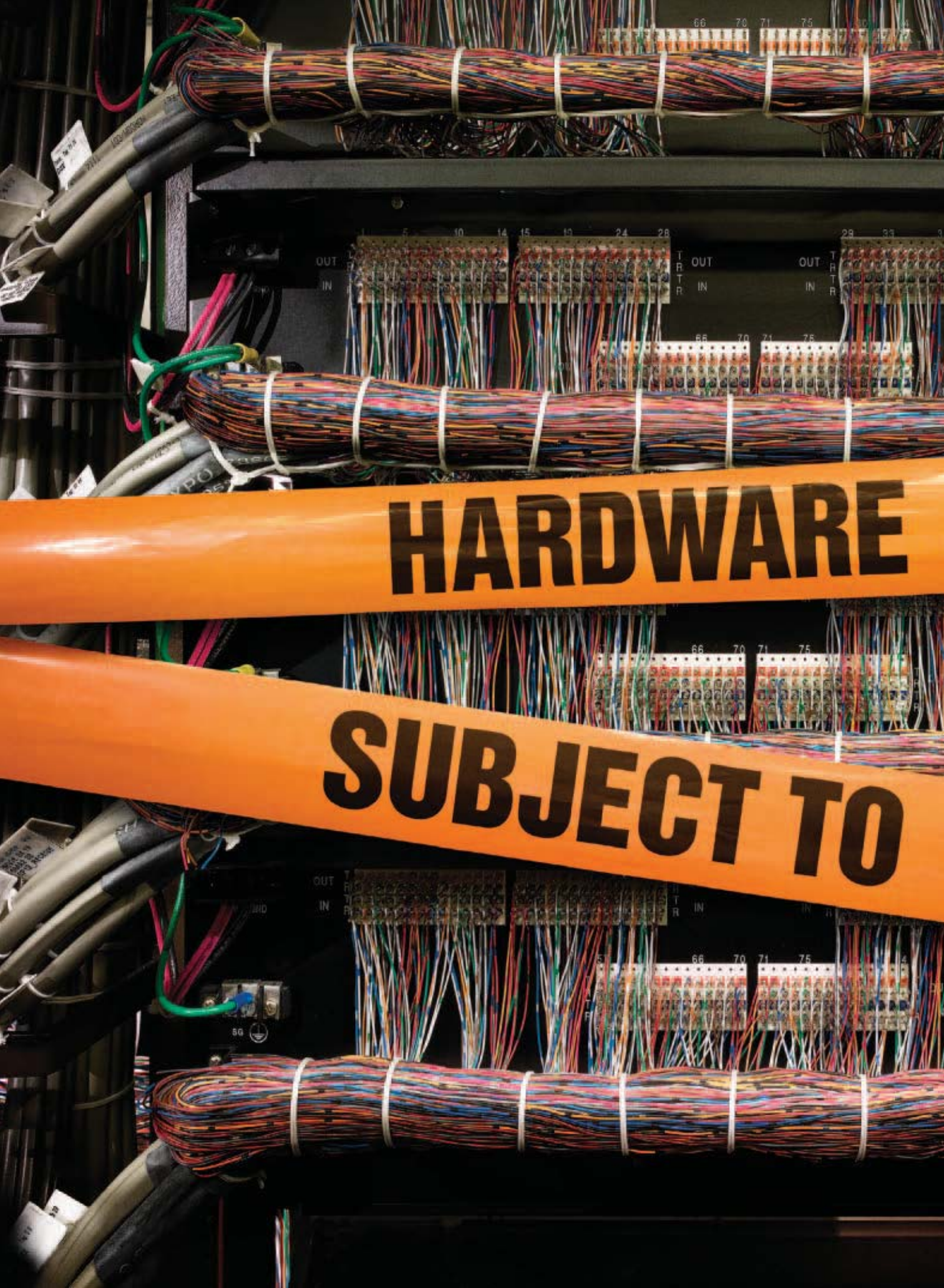
PowerShell 201:
Conditional Statements p. 41

Mark Minasi on Server Core Event Logs p. 16

Top 10:
Steps to Migrate Virtual Machines p. 18

Say "Whoa!" to Runaway Processes p. 19

Penton
A PENTON PUBLICATION
NOVEMBER 2008
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95


HARDWARE
SUBJECT TO



Connect your mobile users without disconnecting your PBX.

Move your mobile workforce over to VoIP using innovative software from Microsoft. Software that integrates with Windows Server® Active Directory® services, Microsoft® Office, and Microsoft Exchange Server. Keep your existing PBX hardware and still get new voice capabilities like drag-and-drop conferencing, anywhere access, and click-to-call functionality from familiar desktop applications.

A software-powered VoIP solution, based on Microsoft Office Communications Server 2007, helps you increase the productivity and flexibility of your workforce—especially your mobile users. Empower your people with better connectivity, leave the PBX plugged in. Learn more at microsoft.com/voip

VoIP AS YOU ARE.

Your potential. Our passion.®

Microsoft®

SBS 2008 AND EBS 2008 REVEALED!

COVER STORY

27 SBS 2008 and EBS 2008 Build on Knowledge Every IT Shop Needs

Microsoft's thorough research into what SMBs need in a network infrastructure led to easier installation and management for the latest version of Windows Small Business Server and the new Windows Essential Business Server.

BY KAREN FORSTER





IT PRO HERO

29 SBS 2008 and EBS 2008: The View from the Trenches

The wizard-based deployment and preinstallation tools that come with Small Business Server 2008 and Essential Business Server 2008 are a hit, but the cost and the migration process are less than ideal.

BY KAREN FORSTER

MORE ON THE WEB

Read these articles at www.windowsitpro.com.

Migrating to Office 2007

If your company is planning a migration to Microsoft Office 2007, you need to consider several key issues, including compatibility, a new interface, and migration challenges.

BY DAN HOLME

InstantDoc ID 100215

SQL Server 2008

IntelliSense and T-SQL debugging; Hot Add CPUs; data compression; new DATE, TIME and spatial data types; and a host of other new features make SQL Server 2008 a must-have upgrade for Enterprise and SQL Server 2000 users.

BY MICHAEL OTEY

InstantDoc ID 100315

C O N

Windows IT Pro

NOVEMBER_2008

VOLUME_14

NO_11

FEATURES



33 Securing Windows Desktops Using Group Policy

Check out how you can use Group Policy's security configuration management features to protect your company's data and systems.

BY DARREN MAR-ELIA

38 10 Reasons to Deploy Windows Vista

The decision to upgrade your XP systems to Vista is simple when you consider features such as easier backup, a great desktop search, and vastly improved security options.

BY MARK MINASI

39 10 Reasons *Not* to Deploy Windows Vista

The decision to upgrade to Vista has to make business sense, but many companies find that training costs and application compatibility problems outweigh any benefits Vista provides.

BY ALAN SUGANO

41 Controlling Your Code's Flow with PowerShell's Conditional Statements

PowerShell's if, for, and while statements let you present conditions and the actions to occur when those conditions are met. You can even specify the actions to occur when a condition isn't met.

BY ROBERT SHELDON



INTERACT

25 Reader to Reader

Document Windows servers with SYDI and use SFU commands to make your batch files more powerful.

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

TENTS

COLUMNS



FORSTER | HEY MICROSOFT!

5 Microsoft's Evolution Toward Software Plus Services

Can Microsoft balance the push toward hosted services with its traditional software products business plan?



THURROTT | NEED TO KNOW

12 Microsoft Internet Explorer 8.0 Features

Internet Explorer (IE) 8.0 is enterprise-friendly, but should you upgrade? Get the scoop on IE 8.0 from Microsoft's Dean Hachamovitch, general manager for the Internet Explorer team.



MINASI | WINDOWS POWER TOOLS

16 Monitoring Server Core Event Logs

Wondering how to monitor a Server Core system's event log? Server Core and Windows Vista offer a powerful command-line event-log query and control tool called Wevtutil that can do it.



OTEY | TOP 10

18 Steps to Migrate VMs from Virtual Server 2005 to Hyper-V

The common VHD format lets you move VMs from Virtual Server 2005 to Hyper-V—follow these 10 steps for an easy migration.



MORALES | WHAT WOULD MICROSOFT SUPPORT DO?

19 Say "Whoa!" to Runaway Processes

Solve performance problems by using two free Microsoft tools to reveal which components within a process consume the most memory.



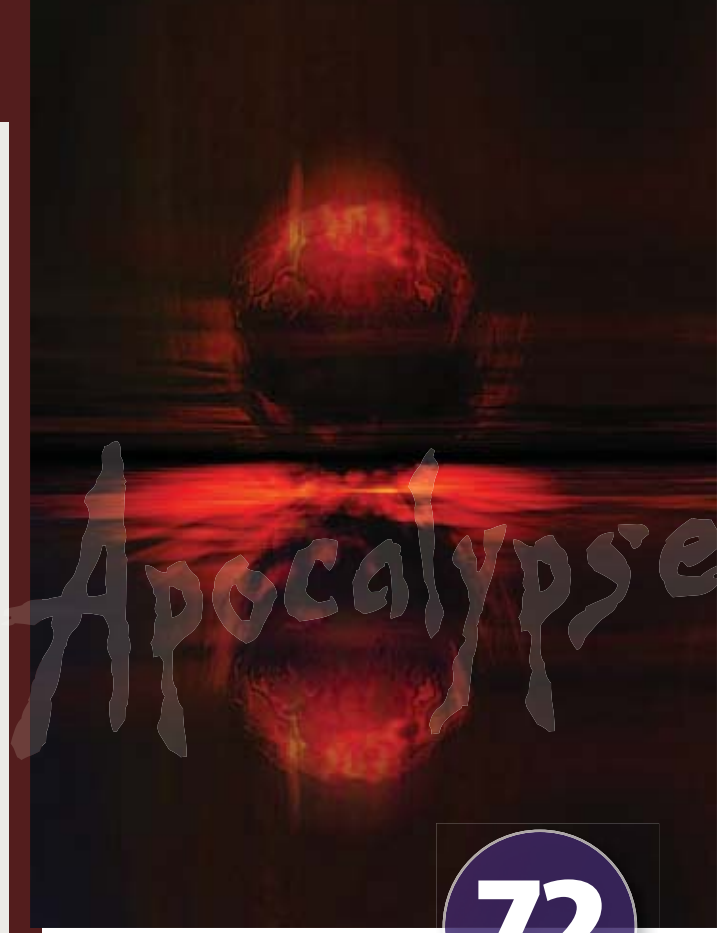
JAMES | EVERYTHING BUT MICROSOFT

51 Who Says You Need Microsoft Exchange Server?

Exchange dominates messaging but can be overkill in small or midsized environments. Alternatives can provide functionality at lower prices without sending your messaging onto the Internet.



"640K ought to be enough for anybody."
- Bill Gates,1981



72

PRODUCTS

48 New & Improved

Check out the latest products to hit the marketplace.
PRODUCT SPOTLIGHT: Ctrix's **XenApp 5**.

COMPARATIVE REVIEW

53 SharePoint Backup Tools

Whether you administer a single SharePoint server or a large farm, there's a backup and recovery solution tailored to your needs.
BY CURT SPANBURGH

BUYER'S GUIDE

59 Enterprise Firewall Appliances

Choose the best firewall appliance to burn up your security threats.
BY JEFF JAMES

64 Industry Bytes

Concern outweighs action when it comes to the environmental impact of electronics; a partnership with HP and ActivIdentity secures multifunction printers; and Clarus Systems introduces its specialized approach to unified communications.

IN EVERY ISSUE



9 letters@windowsitpro.com
10 Your Savvy Assistant
71 Directory of Services
71 Advertising Index
71 Vendor Directory
72 Ctrl+Alt+Del

ALTERNATIVE THINKING ABOUT POWER & PERFORMANCE:

If knowledge is power, then managing it is genius.

It's a simple fact: your system is only as good as the power that runs it. That's why smart power management is crucial. Enter the HP Insight Power Manager, which gives you the ability to control your power and cooling — from forecasting needs to monitoring consumption and lowering energy use. All with the reliability of ProLiant technology. So, while others try to think outside the box — we're rethinking what goes on inside it.

Technology for better business outcomes.

intel Xeon® inside™

Powerful. Efficient.



HP BladeSystem c-Class

- Powered by the Intel® Xeon® Processor
- Infrastructure-in-a-box saves you time, power and money by reducing repetitive parts and redundant operations
- Improves efficiency by managing power and cooling as a resource





HP ProLiant DL Servers

- Powered by the Intel® Xeon® Processor
- Affordable, modular rack systems to give your IT department the flexibility to expand with your business
- Ideal for general-purpose solutions and high-performance computing

To learn more, call 1-877-311-3620 or visit hp.com/servers/rethink49

Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries.
© 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Forster

"The benefit of S+S is that customers have choices."



Microsoft's Evolution Toward Software Plus Services

Survival of the fittest strategy

All Microsoft teams that work on software products insist that they are committed to the Software Plus Services (S+S) strategy. However, some teams are in the odd position of having to support the company's move to the cloud while also being responsible for delivering software-based solutions. A case in point arose when I was preparing this month's cover story on Small Business Server (SBS) 2008 and Windows Essential Business Server (EBS) 2008. I talked to the Microsoft teams responsible for those products and also got input from two SBS MVPs, Susan Bradley and Nick Whittome (see "SBS 2008 and EBS 2008 Build on Knowledge Every IT Shop Needs," page 27, and "SBS 2008 and EBS 2008: The View from the Trenches," page 29). Susan and Nick noted that hosted email sometimes makes more sense for small and midsized businesses than the integrated version of Exchange Server that comes with SBS and EBS. But the Microsoft representatives, while loyally supporting S+S, had to defend the need for Exchange Server as part of their products.

The Microsoft View

Stating Microsoft's position, Devesh Satyavolu (a product manager for the family of Windows Essential Server Solutions, which includes SBS, EBS, and Windows Home Server), said "Microsoft's path towards cloud computing is an evolution, and all products are on that path, including SBS. In fact the version that we're talking about here already integrates with cloud-based services right now."

Guy Haycock (senior product planner for SBS) added, "There are five pieces of new S+S in SBS 2008, compared to none in SBS 2003. I think it's good that Microsoft has multiple choices for small businesses."

And Devesh listed some good reasons for considering software solutions such as SBS and EBS instead of a hosted solution: "If you're in the midmarket, chances are you already have an existing IT infrastructure, a couple of servers. So the first questions to ask yourself are, 'If I'm going to subscribe to some online service, how will that integrate with my existing infrastructure? When I configure a user in my AD on premise, will that [configuration] connect with the cloud?' That's a big question. Second, 'Will the cloud solution automatically provision users, apply patches, and things like that?' Also, if you have a line-of-business application, some mission-critical apps are still not cloud enabled. Next, people are concerned about control. For doctors, there are serious privacy implications. Then there's the question of languages, availability, and support. Finally there's cost. The pros for services are you remove the hassle of maintaining, etc. But I've heard customers say, 'Look, I'm paying this monthly fee and I don't own anything.' It goes back to the question that we're on a path here."

The MVP View

Susan and Nick agreed that different situations will demand different solutions. However, the MVPs added some real-world perspective. Susan noted, "Gartner believes every firm with one thousand seats or less should look to web-based email."

Nick said, "I think that Gartner is correct about small companies looking at web-based email, but they have the [company size] wrong. We are looking more and more at hosted solutions for companies that have under 10 users. Some industry pundits state that all small and medium firms would be best served placing their messaging role in a cloud. I'm not convinced this is right for every firm. But I certainly see the need."

Susan noted, "I'm not sold that web email is the right solution for all clients. Many of us, for paranoia or security reasons, still need on-premises servers."

Nick agreed, "Some firms may wish that the messaging server role was cloud based. However, given retention and legal needs of the firm, an onsite messaging server may be preferable over a cloud-based one. Regardless, to anyone deploying any sort of on-premises messaging server, whether EBS or SBS, I would recommend a cloud-based filtering solution in front of the server. I see the initial interest in this solution being evangelized most by consultants whose firms have outgrown their seventy-five users/devices networks based on SBS 2003."

The Recommendation

In typical Darwinian fashion, Microsoft's new direction toward cloud computing is competing with the traditional software business even while the company insists that the strategies are complementary: It's not software *or* services; it's software *plus* services. The benefit of this forced marriage is that customers have choices. I'd love to hear whether this issue of hosted services versus software products affects your IT decisions. Send me an email and let me know.

InstantDoc ID 100399

KAREN FORSTER (karen@windowsitpro.com) is editorial and strategy director for *Windows IT Pro* and *SQL Server Magazine* and former director of Windows Server User Assistance at Microsoft.

EDITORIAL

Executive Director of Editorial and Strategy, IT Division
Karen Forster karen@windowsitpro.com

Executive Editor, IT Group
Amy Eisenberg amy@windowsitpro.com

Technical Director
Michael Otey mikeo@windowsitpro.com

Web Site Strategic Editor
Anne Grubb agrubb@windowsitpro.com

Executive Editor, Web and Industry
Jeff James jjames@windowsitpro.com

IT Group Managing Editor
Cindy Bushong cindy.bushong@penton.com

Systems Management
Barb Alexy Deputy Editor balexy@windowsitpro.com
Karen Bemowski Senior Editor kbemowski@windowsitpro.com
Caroline Marwitz Associate Editor cmarwitz@windowsitpro.com
Zac Wiggy Assistant Editor zwiggy@windowsitpro.com

Messaging , Mobility, SharePoint, and Office
Gayle Rodcay Senior Editor grodcay@windowsitpro.com
Brian Keith Winstead Associate Editor bwinstead@windowsitpro.com

Networking and Hardware
Jason Bovberg Senior Editor jbovberg@windowsitpro.com

Security
Lavon Peters Senior Editor lpeters@windowsitpro.com

SQL Server
Megan Bearly Keller Associate Editor mkeller@windowsitpro.com
Sheila Molnar Executive Editor, SQL Server and Developer smolnar@windowsitpro.com

Storage, Backup and Recovery
Derek Maness Associate Editor dmaness@windowsitpro.com

Production Editor
Brian Reinholz breinholz@windowsitpro.com

Administrative Assistant
Mary Waterloo mwaterloo@windowsitpro.com

IT Media Group Editors
Erin Bradford
Cassie Deemer
Vicki Hamende
Linda Harty
Chris Maxcer
Rita-Lyn Sanders

ART & PRODUCTION

Senior Art Director
Larry Purvis lpurvis@windowsitpro.com

Art Director
Layne Petersen layne@windowsitpro.com

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Production Manager
Kate Brown kbrown@windowsitpro.com

Assistant Production Manager
Erik Lodermeier erik.lodermeier@penton.com

CONTRIBUTORS

News Editor
Paul Thurrott news@windowsitpro.com

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Joseph Edwards mje@windowsitpro.com
Kathy Ivens kivens@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Jerry Cochran jerryco@microsoft.com
Sean Deuby sdeuby@windowsitpro.com
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond tony.redmond@hp.com
Ed Roth eroth@windowsitpro.com
Eric B. Rux ericbrux@whshelp.com
William Sheldon bsheldon@interknowlogy.com
Randy Franklin Smith rsmith@montereytechgroup.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

CUSTOM MEDIA

Custom Media Director
Michele Crockett mcrockett@windowsitpro.com 970-203-2924

Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Penton
Penton Media, Inc.

Chief Executive Officer
Sharon Rowlands Sharon.Rowlands@penton.com

Chief Revenue Officer
Darrell C. Denny Darrell.Denny@penton.com

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

International Publisher
Jeff Lewis jlewis@windowsitpro.com 970-613-4960

Group Administrative Manager
Danna Varnell dvarnell@windowsitpro.com

Group Interactive Publisher
Peg Miller pmiller@windowsitpro.com

EMEA Managing Director
Irene Clapham irene.clapham@penton.com

ADVERTISING SALES

Director of Sales
Birdie J. Ghiglione birdie.ghiglione@penton.com 619-442-4064

Key Account Directors
Jeff Carnes jeff.carnes@penton.com 678-455-6146
Chrissy Ferraro christina.ferraro@penton.com 970-203-2883
Richard Resnick richard.resnick@penton.com 951-302-2998
Jacquelyn Baillie jacquelyn.baillie@penton.com 714-623-5007

Account Executives
Kelly Koza, Midwest kelly.koza@penton.com 970-203-2932
Barbara Ritter, West Coast barbara.ritter@penton.com 858-759-3377
Cass Schulz, East Coast cassandra.schulz@penton.com 858-357-7649

Client Project Managers
Michelle Andrews michelle.andrews@penton.com 970-613-4964
Kim Eck kim.eck@penton.com 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

REPRINTS

Reprint Sales
Diane Madzelonka Diane.madzelonka@penton.com 216-931-9268 888-858-8851

MARKETING & CIRCULATION

Group Audience Development Director
Marie Evans marie.evans@penton.com

Renewal Marketing Manager
Tricia McConnell tricia@windowsitpro.com

Online Marketing Manager
Anne Oaks anne.oaks@penton.com

Marketing Associate
Christan Humphries christan.humphries@penton.com

Marketing Director
Sandy Lang sandy.lang@penton.com

Marketing Coordinator
Andrea Knudson andrea.knudson@penton.com

Windows®, Windows Vista®, and Windows Server® are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries and are used by Penton Media under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation.

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

PROGRAM CODE
Unless otherwise noted, all programming code in this issue is © 2008, Penton Media, Inc., all rights reserved. These programs may not be reproduced or distributed in any form without permission in writing from the publisher. It is the reader's responsibility to ensure procedures and techniques used from this publication are accurate and appropriate for the user's installation. No warranty is implied or expressed.

LIST RENTALS
Contact Walter Karl, Inc. at 2 Blue Hill Plaza, 3rd Floor, Pearl River, NY 10965 or www.walterkarl.com/mailings/pentonLD/index.html.

SUBSCRIPTION INFORMATION
Subscriptions in US, $54.95 for one year (12 issues for 2008); in Canada, $59 US currency, plus GST for-one year; in all other countries, US $99. Payment should be made in US dollars drawn on US banks. For new subscriptions, call 800-793-5697 or 970-663-4700, or check our Web site at www.windowsitpro.com. For questions or other subscription problems, call customer service at 800-793-5697 or email subs@windowsitpro.com. Europe, europe@windowsitpro.com, *Windows IT Pro*, Di-An House, 2 Aegean Road, Atlantic Street, Altrincham, Cheshire, WA14 5UW, England; tel.-0161 929 2800, fax-0161 929 1511.


Your potential. Our passion.
Microsoft
Data powers your company.
And you're about to turn up the voltage.
Introducing Microsoft® SQL Server® 2008. Harness the power of the data explosion. There's been an explosion in the amount of data, and the number of data formats, in enterprises in recent years. With new SQL Server 2008, you can harness the untapped power of that data explosion by integrating, managing, and delivering that power to your end users. One example: SQL Server 2008 integrates every kind of data you have, from documents to multimedia, from spatial/geographic data to XML. See the power you can give end users at SQLServerEnergy.com
Microsoft®
SQL Server® 2008

Upgrade to Next-Generation Antispam/Antivirus for Exchange.

NINJA™
Email Security for Exchange



Osterman Research: "Half the admin time!"

SC MAGAZINE AWARDS 2007 WINNER
Honored in the U.S.

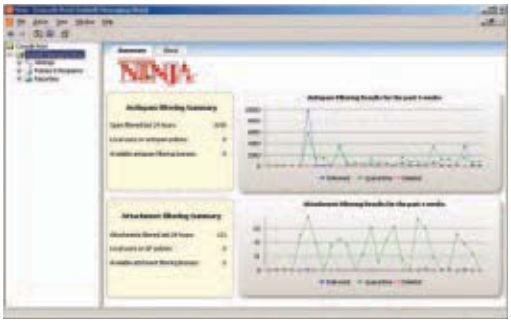
Windows IT Pro READERS CHOICE 2006 Winner

Product Excellence Awards 2007
Info Security Products Guide
CUSTOMER TRUST

Meet Sunbelt Ninja Email Security: The award-winning all-in-one, best-of-breed, third-generation email security solution. Ninja is a plug-in framework that integrates best-of-breed antispam, antivirus, disclaimers and SMART attachment filtering on your Exchange server.

Half the admin time: Independent research shows that Ninja requires one-half the IT time to manage than other comparable email management systems.* With its MMC interface, Ninja is easy to manage so you can get up and running in minutes vs. hours.

Better multi-engine spam detection: Ninja's filtering decimates junk mail and image spam with both Cloudmark (which includes antiphishing) and Sunbelt's own heuristics-based iHateSpam engines. Of course, it also supports RBLs and SPF.



Integrated multi-engine antivirus: Ninja combines the power of multiple high-quality AV engines.

Great end-user control: The policy-based plug-in architecture allows you powerful, granular control. You can finally rule with an iron fist.

SMART attachment filtering: Ninja features the first flexible policy-based attachment filter that isn't fooled by extensions. It looks inside files to determine their true identity. Your policies decide what happens to all attachments.

Download your evaluation copy at:
www.sunbeltsoftware.com/ninjawinb

Sunbelt Software

Email sales@sunbeltsoftware.com or call 888-688-8457 for your 50% discount competitive upgrade quote

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbeltsoftware.com sales@sunbeltsoftware.com

The competitive upgrade is based on 50% of Ninja list price.

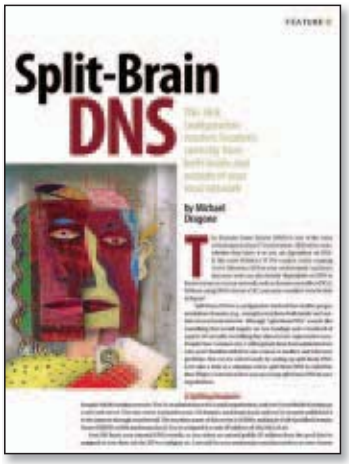
© 2007-2008 Sunbelt Software. All rights reserved. Ninja Email Security and Suspicious Mail Attachment Removal Technology are trademarks of Sunbelt Software. All trademarks used are owned by their respective companies.

*Based on Osterman Research report "Comparing Email Management Systems that Protect Against Spam, Viruses, Malware and Phishing Attacks". December 2006.

- Split-brain DNS
- Thurrott man-crush
- Hyper-V FAQs
- Server 2008 licensing

LETTERS@WINDOWSITPRO.COM

Split-Brain DNS



I read Michael Dragone's "Split-Brain DNS" (September 2008, InstantDoc ID 99772) and found it helpful. However, I have a question about split-brain DNS setup. In my scenario, mydomain.com has an internally hosted web server (WEB01) externally published as www.mydomain.com, as well as an externally hosted web server (WEBSVR05) externally published as webi.mydomain.com. If I use split-brain DNS, I would add only WEB01 to my internal DNS server's mydomain.com zone. So, calling www.mydomain.com should be resolved by WEB01—by querying the address zone mydomain.com. However, if I call for webi.mydomain.com, my DNS server won't find it locally and should forward the resolve call to my ISP's DNS servers and get it resolved there.

As far as I understand the mechanism of a Windows Server 2003 DNS server, that last part won't happen, right? Or can I manipulate certain settings or configurations to achieve this behavior? If not, once I add an Internet-known zone to my internal DNS server, I'll need to add (manually) all servers to this zone. Or can I get a list of all servers of a domain known on the Internet, then import them into the flat file of the new zone (automatically)?

I'm looking for ways to resolve hostnames in domains where we have some servers hosted internally and some hosted externally (with a hosting company).

—Marc Engrie

In the situation you've outlined, you're correct. The DNS server wouldn't forward the query for webi.mydomain.com to your ISP's DNS servers. Note that this behavior isn't specific to the Windows DNS server; it would happen with any DNS server. This situation occurs because the mydomain.com zone is present on the DNS server, making it able to authoritatively answer queries for any host in the mydomian.com zone.

Once you set up my domain.com on your internal DNS server, you'll need to add the appropriate A records for externally hosted hosts. Have the hosting company send you a copy of the zone file. You'll have to edit it to add A records for your internally hosted hosts.

—Michael Dragone

Thurrott Man-Crush

I read Christan Humphries' "Relieve Your SharePoint Pressure Points" (September 2008, InstantDoc ID 99776). The article was informative, well written, and fun to read. I'm looking forward to more from Christan.

I've subscribed to *Windows IT Pro* off and on for a long time. I get overloaded from time to time, and the unread issues start to pile up, so every now and then I back off for a while. But the magazine is too good to be away from for too long. I also have a huge man-crush on Paul Thurrott and really enjoy his podcasts, emails, tweets, and what-not. Recently, I subscribed again because of him.

—jw

Hyper-V FAQs

I read Michael Otey's Top 10 column, "Hyper-V FAQs" (August 2008, InstantDoc ID99440). In the 10th FAQ, Michael addresses whether Hyper-V runs like Virtual Server, on top of Windows. Michael's answer is no. Although all the architecture diagrams I've seen agree with his answer, it would have been a good service to readers to clarify that they must first install the Server 2008 OS before installing Hyper-V.

—George Squillace

You're right. At this time, you still need to install some form of Server 2008 to get Hyper-V. However, Microsoft is planning a standalone version of Hyper-V in the near future.

—Michael Otey

Windows Server 2008 Licensing

I have a question about the sidebar, "Windows Server 2008 Availability and Licensing," which appeared with Paul Thurrott's "Windows Server 2008's Radical New Features" (July 2008, InstantDoc ID 99141). Am I correct in assuming that I can run four virtual instances of the Enterprise edition? Also, if I have a server with VMware ESXi installed and I have a license for Server 2008 Enterprise, can I still use four virtual instances? Or does the license apply only to Hyper-V?

—Virginie Arsenault-Jacques

You're correct: Server 2008 Enterprise provides a license for an additional four virtualized instances of the Enterprise edition. You can run these instances on any virtualization platform, including VMware ESX.

—Paul Thurrott

InstantDoc ID 100336

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

ONLINE

windowsitpro.com

Any DNS Experts Out There?

After reading Michael Dragone's "Split-Brain DNS" article, reader Jeff Krull shared a split-brain DNS configuration problem in the article's comments section. If you think you can help Jeff, log on to www.windowsitpro.com, enter InstantDoc ID 100405, and read about his problem. Then, add your solution! The first reader to solve Jeff's problem will receive a *Windows IT Pro* baseball cap.

Humphries

The missing link to IT resources



ONLINE
windowsitpro.com

Maximize Trust Using Extended Validation SSL

Retain customer trust by learning about Extended Validation (EV) Secure Sockets Layer certificates from Verisign, a leading SSL Certificate Authority vendor. Learn how to shore up weaknesses in your existing system, incorporate EV certificates into current browsers, and manage architectural complexities.
www.windowsitpro.com/go/SSL

Monitor Cross-Platform SOA Performance

Learn about the various methods of monitoring service-oriented architecture (SOA) transaction performance, as well as the pros and cons of each method. Lack of visibility into the entire transaction path and supporting infrastructure, along with the likelihood that some element of every transaction will cross platform boundaries between .NET and J2EE resources, complicates the need to monitor SOA end-user transactions. This on-demand web seminar shows how single-solution SOA monitoring can identify and alleviate response time bottlenecks in a cross-platform Web Services environment.
www.windowsitpro.com/go/CrossPlatformSOA

1-Day Training: SQL Server 2008

Make the Jump—Plan Your Migration! SQL Server 2008 is finally here, but is it worth the upgrade? Drill deep into all the questions about if or when to upgrade. Learn about the pitfalls to watch out for, as well as best practices collected from hundreds of upgrades around the world. Join independent SQL Server experts in 4 U.S. cities for training on everything you need to know about upgrading to SQL Server 2008. Register early for special pricing of $59 through November 14.
www.windowsitpro.com/go/SQLTraining

Virtualization Nation

Finally, you can make a decision based on performance, not promises

After months of events, campaigning, and horn tooting, we'll soon see the results of one of this year's hardest-fought battles. Two contenders—one that's new and touts a fresh perspective; the other born to a heritage of authority and adorned with expectations of greatness—are striving for the same goal: to be your organization's virtualization hypervisor.

That's right; we're not talking about Barack Obama and John McCain. It's Microsoft Hyper-V and VMware ESX Server that are going head to head, without any thrilling (and not-so-thrilling) speeches and forgoing the use of cosmetics on farm animals (at least, let's hope so). With both products' hypervisors now available for free and a Microsoft veteran at VMware's helm, we can only guess what's next in this race to be the best. But for me, at the time of writing this article, I'm preparing to witness the final round of this fight: a throw-down in Denver—a competition of pure performance—from which only one competitor will walk away a winner. (OK, so it's a local event and the user group organizing it prefers the term "neutral comparison," but I still expect there to be a duel to the death—or at least an exchange of unkind words.)

Hype aside, the competition between ESX Server and Hyper-V will continue far beyond the Denver event. Even after your organization has made the move to virtualization, you'll need to deal with virtual machine sprawl, security, and single-point-of-failure difficulties. Avoid being trampled in the virtualization race and those running in (or from) it by equipping yourself with the library of information on WindowsITPro.com, from product reviews to expert commentaries. Read what the Hyper-V camp says about its candidate in Paul Thurrott's web-exclusive article "Microsoft Finally Details Standalone Hyper-V" (InstantDoc ID 100238). For background on ESX Server, see Alan Sugano's web-exclusive "VMware Infrastructure Starter Package" (InstantDoc ID 97037).

For a side-by-side comparison of the products, you can't beat Michael Otey's two-part "Virtualization Shootout" (InstantDoc IDs 98879 and 99248). To stay up-to-date on virtualization, subscribe to the Virtualization UPDATE e-newsletter (WindowsITPro.com/email) for monthly news and developments and join the virtualization forum (WindowsITPro.com/go/VirtualizationForum) for tips from your peers.

For more virtualization Q&A, opinion, how-to, and background articles, see my extended blog post. I'm Your Savvy Assistant, and I approve this message.

InstantDoc ID 100307

October's Web of Articles

WindowsITPro.com provides more articles and topics than we have room for in the magazine. This month, Tony Redmond explains how to connect Microsoft mail clients to Gmail (InstantDoc ID 99782), William Lefkovics shares tips about Outlook (InstantDoc ID 100233), and reader Mauro Magni offers a script that enhances reporting for memory and process information (InstantDoc ID 100059). Also, see my blog at InstantDoc ID 100307 for a guide to this month's bonus content for VIP subscribers!



... Tired of Nursing Your Exchange Server?

#1 BEST SELLER!





Created By

Lucid

Solutions Inspiring Confidence

Anyone who has given birth to an Exchange network knows it can get sick and needs some nursing to stay healthy. In fact, 72% of Exchange Administrators surveyed* have "experienced" an Exchange disaster (feels like the flu)—usually from improper feeding and care.

Like many databases, constant adding and deleting can corrupt an Exchange data file so it eventually turns sour. Replicating, archiving and backing up the data doesn't stop the stink—it just stores it. You've got to…

Fix the Problem

You may have tried the free utilities to fix Exchange. While they help, they are too tedious, time consuming and lightweight to keep your Exchange baby healthy. You've tried the milk, now try some meat!

Pamper Yourself with GOexchange

It's time to try GOexchange, from Lucid8, the #1 best-selling automated disaster prevention and optimization software for Microsoft Exchange 5.5, 2000, 2003 and 2007. As the mother of all Exchange tools, GOexchange helps prevent disasters, repair problems, improves performance, and saves you a lot of time.

"Without routine maintenance, decreasing performance, increased warnings and errors accumulate and database fragmentation transpires, leading to Exchange disasters."

Gartner

Prevent Hiccups

GOexchange removes errors, warnings and inconsistencies within the database—before major corruption makes the database fail.

"GOexchange corrected 2,264 errors and 26 warnings."

Paul Ramos, Director IT

Run, Don't Crawl

In addition to fixing the database, GOexchange removes sluggishness and improves performance by re-indexing and defragmenting the database to permanently remove white space and deleted items. The end result is increased performance and stability with a compact efficient database that's 31 to 55% smaller! Combine this with archiving and the database is up to 91% smaller—making it much quicker to backup.

"..our information stores were reduced by 45-50%."

Dale Huitt, Systems Lead

Automated Babysitter

First, GOexchange is easy to setup and use. Twenty minutes—that's all it takes to get your server up and running. Just schedule it, and walk away!

The software notifies the users, validates the database, runs the backup, conducts a comprehensive system analysis and diagnostics, logs the errors, and notifies you if it discovers a "stop" error—then it repairs and defragments the database, generates a thorough report and schedules the next event.

You can do some of this work yourself, but why waste time doing repetitive maintenance, when GOexchange can do it for you—faster and more effectively than doing it by hand.

"Life before GOexchange…was an absolute nightmare, late nights, long weekends and upset users."

Marty Grogan, CTO

Stop The Crying

Why not call now, or visit our resource site and learn how to reduce the risk, and avoid the pain. Protect your exchange data, maximize performance, and spend a weekend at home—*instead of babysitting Exchange.*

Special Offer

- Free Software for analysis of your Exchange server!
- Free White Paper—"Basic Feeding of Your Exchange Server."
- Free Essential Guide to Exchange Preventative Maintenance

Go to: www.Lucid8.com/GoITPro
Call 425.456.8474
E-mail: Sales@Lucid8.com

Copyright © 2007 Lucid8. All rights reserved. Microsoft® Exchange Server is a registered trademark of Microsoft® Corporation. All other trademarks are the property of their respective owners. * Refers to Survey conducted by Lucid8. See press release for more details.



Thurrott

"While IE 8.0's new features are certainly welcome from an end-user perspective, I would advise enterprises to delay deploying IE 8.0."

Microsoft Internet Explorer 8.0 Features

With the Beta 2 release of Microsoft Internet Explorer (IE) 8.0 delivered to customers in August 2008, Microsoft is on track to ship the final version of its next browser. IE 8.0 delivers on the key tenets of its predecessor, IE 7.0, with advances around day-to-day usage, trustworthy computing and safety, and developer features. But IE 8.0 also includes the biggest technological break with the past yet seen in Microsoft's browser platform: Unlike previous versions, IE 8.0 will render web pages in a standards-compliant mode that's similar to how browsers such as Mozilla Firefox render web pages, a change that could lead to compatibility issues for businesses. Here's what you need to know about IE 8.0.

Improved Browsing

With the industry moving to a cloud computing model where more and more of our work is performed through the web browser, products such as IE are more important than ever before. This increased reliance on the web requires new levels of performance, reliability, and functionality, and, for the enterprise, suitability for mission-critical applications, manageability, and compatibility.

From a raw performance standpoint, Microsoft has tweaked IE 8.0 to make it perform faster. The browser starts up quicker than its predecessor, as do new tabs and secondary windows. Sites with JavaScript will run more quickly as well, Microsoft says, thanks to an overhauled JavaScript parser. Microsoft has also dramatically improved memory management.

Dean Hachamovitch, Microsoft's general manager for the Internet Explorer team, told me that the performance improvements in IE 8.0 go well beyond pure benchmarks, however. "With IE 8.0, the sum is greater than the parts," he said. "We've looked holistically at how users actually use the browser. And we've made sure that IE 8.0 performs better in day-to-day use, making users more efficient and placing them in control."

To this end, IE 8.0 includes hundreds of improvements and small efficiencies. "Accelerators" pop up as needed, giving users context-sensitive actions (formerly called "Activities" in IE 8.0 Beta 1), while "Web Slices," also introduced in Beta 1, provide a way for users to subscribe to portions of web pages that change frequently. (To learn more about IE 8.0 Beta 1, see "What You Need to Know About Microsoft Internet Explorer 8.0 Beta 1," InstantDoc ID 98795.)

The new IE 8.0 Smart Address Bar presents an organized drop-down list that changes as you type, providing you with quick access to your relevant browser history, Favorites, and subscribed RSS feeds. And if one of the search results contains a typo, you can now remove it from your history and thus any future search results. "Our research shows that 80 percent of navigation is to previously visited places," Hachamovitch said.

Tabs, a strong point in IE 7.0, become more intelligent and useful in IE 8.0, which automatically collects related tabs into groups, each of which has its own color scheme. Thus, when you CTRL-click on a link on the current page, the new tab opens next to that tab, and not at the end of the list of tabs; the two tabs also match in color.

"This seems like a small thing, but it's important," Hachamovitch told me. "Tabs open near their source and are grouped according to what the user is doing. They're not just a bunch of tabs, because the user has a task in mind."

And if you open a blank new tab, you're presented with a useful UI that provides access to lists of recently closed tabs (in case you mistakenly closed something important), Accelerators, and other features. You can also bookmark a tab group and then display the group as tabs again later.

Answering one of my long-standing complaints about IE, Microsoft has finally replaced the Find dialog box—which could often obscure the content on the very page you were trying to search—with a new Find On This Page toolbar that appears right below the tabs and Command Bar in the browser's UI. This toolbar offers the option of highlighting search results and works much like a similar feature in Mozilla Firefox. (Now if Microsoft would only add a similar feature to its Office applications, they'd really be on to something.)

The IE 8.0 search box has been dramatically improved, and it applies whether you use Microsoft's Live Search engine or not. The box provides a plug-in model for search providers to create visual search results, so images can appear in-line in the box's drop-down list box, which Figure 1 shows, a feature that's used to great effect by Amazon, among others. And thanks to this new drop-down list, you can easily redirect a search to different providers, moving from, say, Google to Wikipedia with the click of a button. As always, Microsoft lets you keep your default search providers, so if Google is the default before you upgrade, it will still be the default.

On the reliability front, IE tabs and windows now all run in their own processes, so if something in one tab crashes, the crash affects only that one tab. "Crash recovery is great," Hachamovitch said, "But why not just contain the crash and not end up in that situation in the first place? We think of it as Browser NT," a comment that should draw

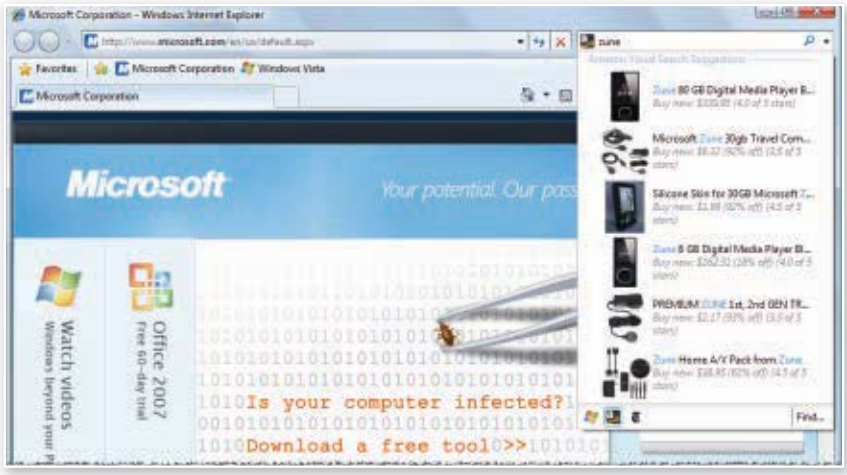


Figure 1: IE 8.0's visual search results

more than a few smiles from the enterprise crowd.

The Links toolbar, widely misunderstood by users of previous IE versions, has been revamped and renamed the Favorites toolbar. It's now used to save RSS feeds and Web Slices, two content types that update frequently and are now more discoverable. Aside from being readily available in the IE 8.0 UI, items in the Favorites toolbar are also bolded when they've been updated.

Enterprise Features

Unlike Mozilla Firefox, IE 8.0 is enterprise-friendly. It can be deployed using standard Microsoft products such as Active Directory (AD), Windows Server Update Services (WSUS), or System Center Configuration Manager 2007 (SCCM), and it can be slipstreamed into Windows client and server installation images. A new version of the Internet Explorer Administration Kit (IEAK) provides pre- and post-installation management of the application, including the ability to configure hundreds of new IE 8.0–specific features via over 100 Group Policy settings. You can also manage compatibility issues by using IE 8.0's new version of the Application Compatibility Toolkit (ACT). And on intranets, IE 8.0 defaults to IE 7.0 rendering mode.

Microsoft will support IE 8.0 with updates for the duration of the life cycle of the OS on which it's installed. And unlike with other browsers, IE 8.0 updates can be managed and configured centrally using existing Microsoft management technologies such as AD, SCCM, and the like.

Safety and Security

Some IE 8.0 security features were revealed with Beta 1, such as the SmartScreen Filter, Cross-Site Scripting Filter, enhanced Delete Browsing History, domain name highlighting, and data execution prevention (DEP) support. Beta 2 shows more changes made since then as well. (See "What You Need to Know About Microsoft Internet Explorer

ISV Innovation

Get on the case

www.getonthecase.com

The need for knowledge drives us. Begin training now at www.getonthecase.com, and become a master of Microsoft® SQL Server® 2008. You'll learn to control powerful new features, taking your skills to the next level.

Your efforts will be rewarded. Prove your heroic new abilities in our game, and you could win an incredible prize. You'll need dedication, intelligence, and intuition. Are you up to the challenge?

For terms and conditions, visit www.getonthecase.com



Microsoft

8.0 Beta 2," InstantDoc ID 99754 for more information.)

Many new security features can be accessed via a new Safety menu item in the IE 8.0 Command Bar. "There are just so many safety enhancements, we had to add that," Hachamovitch told me. "For example, Delete Browsing History is good functionality, but it can be frustrating if you don't want it all wiped out. Now, we protect web site data for sites in your Favorites list by default. But you can also configure exactly what gets wiped out when you use this feature."

A major new feature called InPrivate Browsing lets the user open a separate IE window that won't later reveal any of the browsing history or information that was transacted while open. Hachamovitch called this "over the shoulder" security: The browser history, temporary Internet files, forms data, cookies, and any usernames and passwords aren't stored after the window is closed.

InPrivate Browsing is for those times when you want to keep your activities secret, such as when you're buying a present for the boss. "Buy the present and then just close the window," Hachamovitch added.

InPrivate Browsing also enables a secondary safety feature called InPrivate Blocking that prevents web sites from sharing cookie data about the user with third-party sites. This feature is aimed at protecting the privacy of the user and can be enabled separately from InPrivate Browsing as well.

IE 8.0 also makes it easier than ever to remove browser toolbars, with an always-on "close" box on the left of every toolbar. If you suddenly find that an unrelated software installation has added a toolbar, just close it: IE 8.0 will even prompt you to disable any related browser helper objects as well.

New Developer Features

IE 8.0 will run in a standards-compliant mode by default, which could cause compatibility problems. It has a Compatibility View, which replaces the temporary Emulate IE 7 toolbar button from Beta 1. Exposed as an icon on the right side of the IE 8.0 Smart Address Bar, this feature lets you run IE 8.0 in backward compatibility mode on a site-by-site basis, without requiring browser restarts.

Additionally, developers can specify which of IE 8.0's three rendering engines are used by adding a small bit of code to their sites. In this way, web sites and intranets can force IE 8.0 to render correctly based on their own needs.

Recommendations

My pre-release testing of IE 8.0, using a late beta version, has revealed many compatibility issues, but it's likely Microsoft will resolve them. Most businesses would be wise to at least begin evaluating IE 8.0; however, I would advise enterprises to delay deploying it and to utilize a schedule that's similar in length and scope to that used for an OS service pack.

InstantDoc ID 100199

PAUL THURROTT (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Top 5
Reasons to Advertise with the *Windows IT Pro* Network

5 *Windows IT Pro* is the leading independent voice in Windows IT, reaching 2.5 million engaged users each month.

4 68% of readers spend an hour or more reading each issue.

3 49% of *Windows IT Pro* subscribers visit windowsitpro.com on a monthly basis.

2 On average, each issue of *Windows IT Pro* is passed along to one other colleague.

1 94% of our readers are involved with purchasing, with 74% specifying or recommending brands and suppliers.

Readex Reader Survey, September 2007

Windows IT Pro
www.windowsitpro.com

Contact info:
Birdie Ghiglione
619-442-4064
Birdie.ghiglione@penton.com



What would you do if you had the chance to run Microsoft?

Oh, the power. Ideas you would develop. Products you would kill. Policies you would change. Alliances you would form. Companies you would build, buy, or crush...

Without a doubt, Microsoft is one of the most powerful forces in technology today, and everyone seems to have an opinion about what the Redmond giant does. What's yours?

The 2008 ITTV "If I Ran Microsoft" Video Contest is your chance to tell it like it is.

The first 250 entrants earn a free T-shirt just for participating (one per video), plus are entered to win one of three 8GB Zunes to be given away.

Visit www.ittv.net today

for video contest rules and all the details. Or stop by our booth at Connections in Las Vegas, Nov. 11-13, 2008, to submit your entry. Contest ends Dec. 31, 2008.

ITTV. Don't just watch IT—live IT.

www.ittv.net

Windows IT Pro

SQL Server magazine

ittv.net



Minasi

"You don't want to waste your life analyzing gazillions of event-log entries."

Monitoring Server Core Event Logs

Wield powerful command-line event-log control with Wevtutil

Now that Windows Server 2008 Server Core has been available for half a year, I've had the chance to talk to a lot of people about it. Some people flatly disbelieve that anyone would try to run a CLI-based server. Recently, someone asked, "How can you 'run' a server when you can't see how well or badly it's running?"

Remember, although Task Manager is a GUI tool, it's one of those GUI tools (like Notepad and Regedit) that will run in Server Core's very simple GUI. But what about monitoring a Server Core system's event log? Clearly, the Microsoft Management Console (MMC) Event Monitor snap-in doesn't work on Server Core, but Server Core (and Windows Vista) sports a powerful command-line event-log query and control tool called Wevtutil (wevtutil.qe), which dumps events from any log.

The command's syntax is best described through example:

```
wevtutil qe system /c:1 /rd:true /f:text
```

This command queries (*qe*) the system (*system*) event log, displays the first event (*/c:1*), starts from the most recent event and works backward (*/rd:true*, which means "reverse direction" or "start from the most recent events"), and displays the data as text (*/f:text*) rather than as XML.

You don't want to waste your life analyzing gazillions of event-log entries, so you'll need some sort of filtering ability to separate the wheat from the chaff. To specify query filters, you can add a parameter with an *xpath* query, as in

```
"/q:*[System[(<xmlvalue=value>)]]"
```

For example, if you wanted to see all the so-called heartbeat messages that appear in the event log announcing how long the system has been up, you'd type

```
wevtutil qe system "/q:*[System [(EventID=6013)]]" /f:text
```

I didn't include either /c: or /rd: because I wanted to see all the events and didn't care about the order in which I got them. I constructed the query text "EventID=6013" by looking at a large dump of event-log entries where I *didn't* include the /f:text parameter and so got tons of XML-encoded event dumps. A small excerpt looked like

```
<EventID Qualifiers='32768'>6013</EventID>...<Level>4</Level>
```

Comparing those snippets of XML to their text version told me first that the XML attribute name for the event ID was EventID, and ID 6013 corresponded to the system-uptime messages. Notice the XML attribute Level: A brief comparison with the text version of event-log entries showed me that a Level value of 4 meant *information*, 3 meant *warning*, 2 meant *error*, and 1 meant *critical*. (There are also events with Level values of 0, but in my experience you find them only in the security logs; they're the audit-success and audit-failure entries.)

To see just the critical event log entries in the system log, I'd type

```
wevtutil qe system "/q:*[System [(Level=1)]]" /f:text
```

By including "and" or "or" in your query criteria, you can see both the *critical* and *error* log entries:

```
wevtutil qe system "/q:*[System [(Level=1 or Level=2)]]" /f:text
```

I know; this all looks a bit difficult. Fortunately, there's a way to cheat. Suppose you want a filter for the security log that will show you only audit failures and audit successes. To do that, you'd go to a Server 2008 or Vista system with the full GUI working. In the GUI-based Event Viewer, you'd right-click the security log, choose *Filter current log*, and form the query you want, through the GUI. Then, you'd click the XML tab on the Filter Current Log dialog box. Doing so would yield something like the following:

```
<QueryList>
  <Query Id="0" Path="Security">
  <Select Path="Security">*[System[band(Keywords,
  13510798882111488)]]</Select>
  </Query>
</QueryList>
```

All you need to do is grab the bracketed portion of the third line, make an RDP connection to the Server Core system, and paste the code into a Wevtutil query to get the following:

```
wevtutil qe Security "/q:*[System[band(Keywords,13510798882
  111488)]]"
```

Of course, I could then add /c:, /f:, and other options, but that would do the trick.

InstantDoc ID 100108

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books , including *Administering Windows Vista Security: The Big Surprises* (Sybex). He writes and speaks around the world about Windows networking.

Virtualization is only half the battle for efficiency.

InfraStruXure®
DATA CENTERS ON DEMAND



Principles of InfraStruXure® High Density-Ready Architecture...

1. Rack enclosures that are HD-Ready
2. Metered PDUs at the rack level
3. Temperature monitoring in the racks
4. Centralized monitoring software (not shown)
5. Operations software with predictive capacity management (not shown)
6. Efficient InRow® cooling technology
7. UPS power that is flexible and scalable

Virtualization is here to stay.
And it's no wonder – it saves space and energy while letting you maximize your IT resources. But smaller footprints can come at a cost. Virtualized servers, even at 50% capacity, require special attention to cooling, no matter their size or their location.

1. **Heat** Server consolidation creates higher densities – and higher heat – per rack, risking downtime and failure.
2. **Inefficiency** Perimeter cooling can't reach heat deep in the racks. And over-cooling is expensive and ineffective.
3. **Power Events** Virtual loads move constantly, making it hard to predict available power and cooling, risking damage to your network.

The right-sized way to virtualize.
With the new HD-Ready InfraStruXure architecture, you can take on high-density by cooling the virtualized high-density row, controlling power at the rack level, and managing the system with advanced software and simulation. Though virtualizing saves energy, true efficiency also depends on the relative efficiencies of power, cooling, and servers. Right-sizing one and not the others (See Figure 1) leaves efficiency savings on the table. To right-size, depend on the efficient, modular HD-Ready InfraStruXure and neutralize heat at the source. Equipment will be safer and more efficient running closer to 100% capacity.

Don't agonize, virtualize.
What are you waiting for? With HD-Ready InfraStruXure architecture anyone can virtualize… anytime, anywhere. Just drop it in and go.

Why do leading companies prefer InfraStruXure 6 to 1 over traditional data center designs? Find out at www.xcompatible.com



You can deploy high-density racks right now...

Deploy InfraStruXure as the foundation of your entire data center or server room, or overlay into an existing large data center.

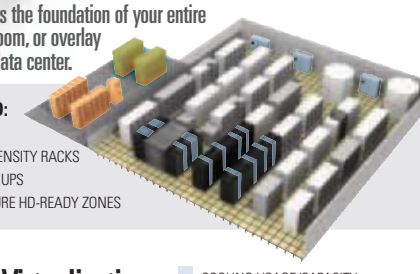


Figure 1

Efficiency and Virtualization

Your servers are efficient, but is your power and cooling?

COOLING USAGE/CAPACITY
SERVERS
POWER USAGE/CAPACITY

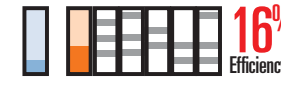
Pre-Server Virtualization
Big gains could be made with both server and power and cooling.

- ☐ Correct Server Utilization
- ☐ Correct-sized Power
- ☐ Correct-sized Cooling



Post-Server Virtualization
Grossly oversized power and cooling cancels out potential gains made by virtualizing.

- ☑ Correct Server Utilization
- ☐ Correct-sized Power
- ☐ Correct-sized Cooling



Server Virtualization with Power and Cooling
Right-sized power and cooling tip the balance back in your favor.

- ☑ Correct Server Utilization
- ☑ Correct-sized Power
- ☑ Correct-sized Cooling



Tested and Approved for InfraStruXure®

The following have been tested and work best with InfraStruXure Solutions. Go to www.xcompatible.com to learn more.

SQUARE D · t.a.c · DELL · CISCO PARTNER Technology Developer · Microsoft · PELCO · IBM ALLIANCE PARTNER · EMC² SELECT



Download a FREE copy of APC White Paper #126:
"An Improved Architecture for High-Efficiency, High-Density Data Centers"

Visit www.apc.com/promo Key Code d928w • Call 888-289-APCC x8029 • Fax 401-788-2797

APC® by Schneider Electric

©2008 American Power Conversion Corporation. Al trademarks are owned by Schneider Electric Industries S.A.S.. American Power Conversion Corporation or their affiliated companies.
e-mail: esupport@apc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA 998-0899_alt



Otey

"When you've got the .vhd file on the Hyper-V system, you might think you're finished, but you aren't."

Steps to Migrate VMs from Virtual Server 2005 to Hyper-V

Avoid the gotchas and have a smooth migration with this simple guide

You've probably heard a lot about how much better Microsoft's new hypervisor-based Hyper-V virtualization is than Microsoft Virtual Server 2005's hosted virtualization. You've also probably heard that the Virtual Hard Disk (VHD) format shared between them makes it possible to move virtual machines (VMs) from Virtual Server 2005 to Hyper-V. However, there are a few gotchas that you need to look out for along the way. Here are the 10 essential steps to migrating your Virtual Server 2005 VMs to Hyper-V.

1 **Make sure the guest OS is at the correct service pack level—** Windows Server 2003 is undoubtedly the most common guest OS, but you need to make sure you've installed SP2 before you migrate. You can find the list of all supported Hyper-V guest OSs, and their service pack levels where appropriate, at www.microsoft.com/windowsserver2008/en/us/hyperv-supported-guest-os.aspx.

2 **Uninstall Virtual Machine Additions—**If you don't remove the Virtual Machine Additions component from the VM guest, you might be stuck with an uninstallable program that prevents you from later installing Hyper-V's integration components. You avoid this error if you've installed Virtual Server 2005 R2 SP2, but it's safer just to remove the component before migrating the VM. You should also note the VM's configuration if you don't already know it.

3 **Shut down the VM—**With the preliminaries out of the way, you're ready to move the VM. First, shut down the VM using the Shut Down option on the Start menu inside the guest. Be sure you shut down the OS instead of saving its state. After the guest OS has shut down, power off the VM from Virtual Server Manager.

4 **Set up a share on the Hyper-V server—**VMs are typically too big to copy on standard media such as USB drives or DVDs. The easiest way I've found is just to share the directory on the Hyper-V system on which you store your Hyper-V VHDs.

5 **Copy the VHD to the target Hyper-V system—**After creating the share, copy the .vhd file to the Hyper-V system. Depending on the size of the file and the speed of the disk subsystem, this process could take a couple minutes. For one-off migrations, I usually use Windows Explorer; if I'm moving multiple VHDs, I use Robocopy.

6 **Create a new Hyper-V VM—**When you've got the .vhd file on the Hyper-V system, you might think you're finished, but you aren't. The VHD contains the stored OS and data for the guest, but it doesn't contain the VM configuration information, such as how much memory the VM has or how many hard disks or virtual network adapters it has. Your best course to move this information is to select New, Virtual Machine from the Actions pane of the Hyper-V Manager to start the New Virtual Machine Wizard.

7 **Add Hyper-V networking to the new VM—**You connect the new VM to the correct network through the wizard. The Virtual Server 2005 virtual networking configuration isn't migrated as part of the .vhd image. On the New Virtual Machine Wizard's Configure Networking page, select the Hyper-V virtual network to which you want your VM's virtual network adapter connected.

8 **Attach the migrated VHD to the new Hyper-V VM—**The trick to migrating the old VHD to Hyper-V lies in linking the .vhd file to the new Hyper-V VM that you've created. On the New Virtual Machine Wizard's Connect Virtual Hard Disk page, select *Use an existing virtual hard disk*, then point the new VM to the VHD you copied from Virtual Server 2005 by entering or browsing to the VHD's path.

9 **Start the new VM—**After completing the wizard, you can start the new Hyper-V VM. Don't be surprised if you're greeted by the annoying Windows Activation screen. Nothing has really changed in the guest, but this screen prevents you from seamlessly moving VMs between Virtual Server and Hyper-V.

10 **Install Hyper-V integration components on the new VM—**Although you previously selected the virtual networking configuration for the VM, you'll need to install the Hyper-V integration components by connecting to the VM, then selecting the Action, Insert Integration Services Setup Disk from the menu to provide the guest with the drivers it needs to use Hyper-V's new synthetic video and networking devices.

InstantDoc ID 100089

MICHAEL OTEY (mikeo@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

Morales

"To troubleshoot processes that consume large amounts of CPU clock cycles, we use two main tools: Process Explorer and Adplus."



Say "Whoa!" to Runaway Processes

Find and resolve CPU-hogging runaway processes using the Process Explorer and Adplus tools

As a Microsoft escalation engineer, I've fielded many calls about runaway processes—a common cause of PC performance problems. You probably already know what a runaway process is: It's a process that consumes one or more processors, causing your system to become sluggish and sometimes causing other applications to freeze or crash. Often you can find such problems quickly by using Task Manager to view information about running processes. The common way to "solve" a runaway-process problem is to just kill the process, but this is only a temporary fix; the runaway process will likely recur.

To truly fix the problem, you might need to enlist the application manufacturer's tech support. However, before you pick up the phone, there are things you can do to make the support call a lot shorter or perhaps avoid it altogether. I'll tell you about a couple of free tools that Microsoft Support uses to troubleshoot runaway processes and show how you can use them to do the same thing at your site.

Two Troubleshooting Tools

To troubleshoot processes that consume large amounts of CPU clock cycles, we use two main tools: Process Explorer and Adplus. Each tool has its advantages and best-use scenarios. Process Explorer is available at live.sysinternals.com. This is the perfect tool to use when you're seeing warning signs that a process will become a runaway and you have either remote or physical access to the system. Adplus is a script file and comes installed with the Debugging Tools for Windows (www.microsoft.com/whdc/devtools/debugging/default.mspx). This is the tool of choice if you don't know exactly when the process will start to run away and you don't have console access when the problem happens.

Using Process Explorer

Here's an actual case from the Microsoft Escalation Services files that shows you how to use these tools. We recently resolved an issue where the Windows XP SP2 wmiprvse.exe process (a separate host process for WMI providers) was spiking the CPU. The customer had already used Performance Monitor, choosing the %Processor Time counter for the wmiprvse.exe process, to identify which process was spiking the CPU.

In this scenario, we knew when the problem would occur, and the customer had physical access to the workstation when the process spike occurred, so our next step was to use Process Explorer to learn more about what components were involved during the spike.

After you've opened Process Explorer, your next step is to configure the location of symbols in Process Explorer. Symbols are used to convert binary information into a readable format. (I discuss symbols in more detail in "Resolve Memory Leaks Faster," October 2008, InstantDoc ID 99933.) But before you configure the symbols' location, make sure that the Debugging Tools for Windows are already installed on your system; you'll use part of this toolset to make your examination of the suspect process seamless.

To configure the symbols' location, in Process Explorer click Options, then click Configure Symbols. If you installed the debugging tools in the default location, the Configure Symbols dialog box should display the symbol path.

Now you're ready to dig into the components within the process that are involved in spiking the CPU. From the list of processes displayed in Process Explorer, locate the spiking process (wmiprvse.exe) and double-click it. You'll see the process's Properties dialog box, which contains all the threads inside that process with the thread consuming the most CPU resources at the top of the list. Next click the Stack button to get the module and function-call listing for the highest–CPU-consuming thread. You'll see a screen like the one that Figure 1, page 20, shows.

In Figure 1 you can see several modules, and you can use their information to start narrowing down the component (or components) that could have caused the runaway process and possibly solve the problem by researching it online. For example, I did a web search on the string "Assetadvisor.dll wmiprvse cpu" because the CPU spike occurred inside the wmiprvse.exe process and Asset Advisor.dll was a component on the stack and repeated several times. My search found a TechNet article providing a fix for the problem at support.microsoft.com/kb/937882. Thus, when you select components to search, you'll probably be most successful searching those that are both high on the thread stack and repeated. Identifying what components are involved in a spike will help you in researching the problem on your own or minimizing the length of a support call, if one is needed.

Remember that Process Explorer worked in our scenario because of two specific conditions:

- We knew when the process would spike the CPU.
- We had access to the affected system's console.



Figure 1: Module and function-call listing for highest–CPU-consuming thread

Using Adplus

If your runaway-process scenario doesn't match both of those conditions, you'll want to consider using Adplus. Adplus lets you gather the same type of information as Process Explorer, but you don't need to know when the process will spike the CPU or have physical access to the system during the problem. I'll demonstrate a quick example using our wmiprvse.exe scenario. You can find more information about how to use Adplus in the Microsoft article at support.microsoft.com/kb/286350/en-us.

Adplus is a .vbs script file that comes installed with the Debugging Tools for Windows and must be run from the directory that the debugging tools are installed in (C:\program files\Debugging Tools For Windows). When you execute Adplus using the correct command-line arguments, the tool will monitor a process and create a dump file when that process spikes the CPU. The following command causes Adplus to monitor the wmiprvse.exe process and create dump files in the c:\dumpfiles directory:

```
C:\Program Files\Debugging
Tools for Windows (x86)>
adplus -hang -pn wmiprvse
.exe -o c:\dumpfiles
```

(The command wraps over several lines because of this magazine's format requirements, but you should type it on one command line.) The -hang switch puts Adplus into Hang mode, which produces full memory dumps for the process specified on the command line after the script has finished. The -pn switch tells Adplus which process to monitor. The -o switch followed by a folder location tells Adplus which directory to store the dump files in.

After the command has run, Adplus will automatically create dump files in the specified directory when the process spikes the CPU. If that directory is shared, you can choose to access it from a remote workstation to see whether Adplus created any files and review them at your convenience.

You can review the dump files created by Adplus for information about runaway processes by following these steps:

1. Run windbg.exe from the Debugging Tools for Windows directory. You'll see a screen like that in Figure 2.
2. Click File-Open Crash Dump and point to the directory containing the Adplus dump files.
3. Select one of the dump files created by Adplus; the file will have a .dmp file extension.
4. From the Windbg prompt, enter *!runaway*. This command outputs the thread consuming the most CPU time. In our example, this is thread 5.
5. To change the context of the debugger to focus on thread 5, enter the command *~5s*.
6. Now run the kv command to get the list of modules and function calls involved in causing the process to spike.

The results of the Windbg commands you entered in the preceding steps point to the same module that we found to be involved when we used Process Explorer (Asset Advisor.dll).

More Options

Which tool you use for troubleshooting runaway processes will depend on your circumstances. Process Explorer is easier to use but won't work under certain conditions. Using Adplus involves more steps but is an option when you can't use Process Explorer—and it provides the same troubleshooting information. The next time you have a runaway process bogging down a system, try one or both of these tools, and let me know how they worked for you!

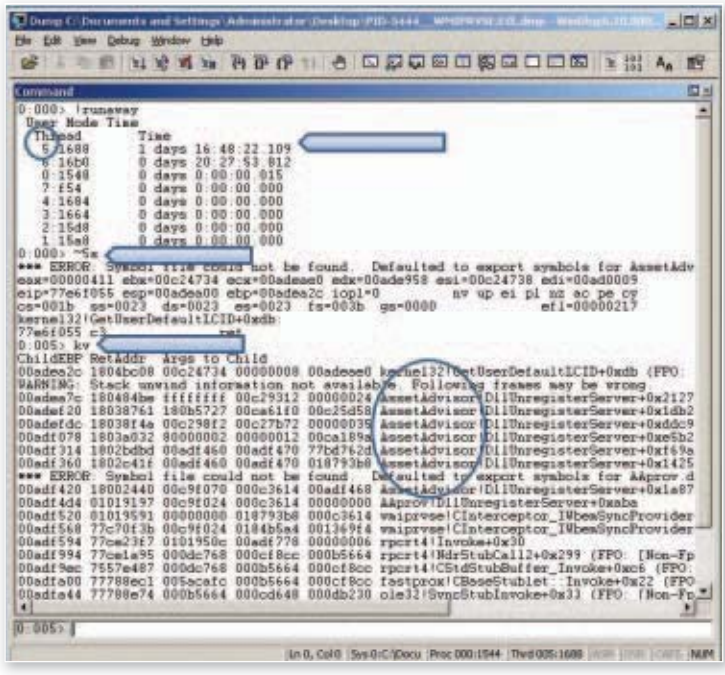


Figure 2: Opening an Adplus dump and running debugging commands

InstantDoc ID 100212

MICHAEL MORALES
(morales@microsoft.com) is a senior escalation engineer for Microsoft's Global Escalation Services team. He specializes in advanced Windows debugging and performance-related issues. For information about Windows debugging, visit blogs.msdn.com/ntdebugging.



Every IT device on your network; including firewalls, servers, routers, phone systems, PCs and more, creates a log with each and every event – resulting in millions of scattered and fragmented audit trails around your network which are impossible to view and analyze as a whole.

GFI EventsManager is a simple to use events management solution that consolidates all security events into a single database and provides advanced alerting, comprehensive reporting and a range of search and drill down tools. These tools deliver insight into all that is happening on your IT infrastructure, allowing full network-wide auditing, also enabling GFI EventsManager to act as an early-warning system for all potential hardware and software failures while ensuring maximum network uptime and monitoring and alerting on possible security breaches from a central location.

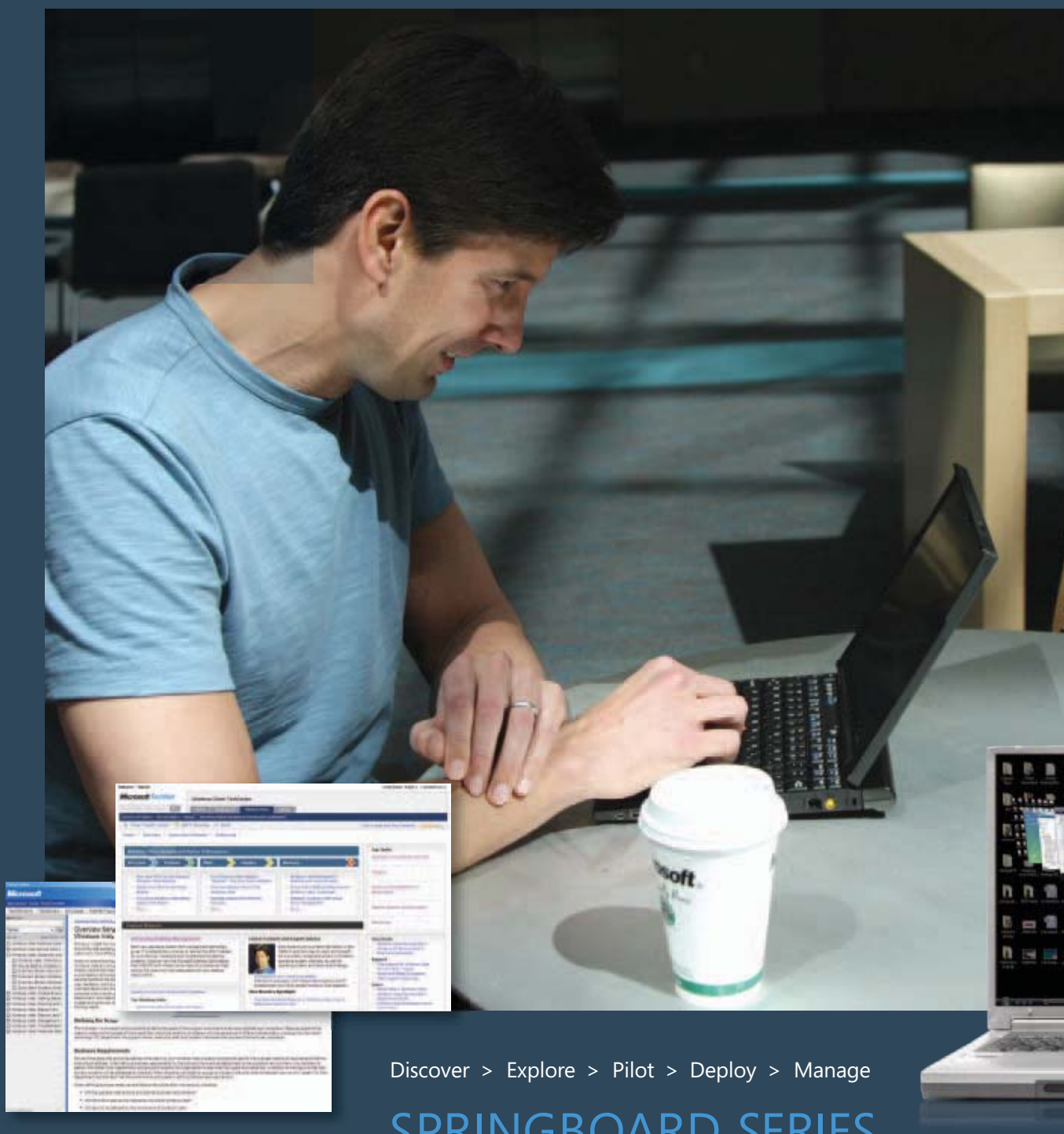
Proper log management helps you to meet several objectives including:

- Information system and network security
- System health monitoring
- Legal and regulatory compliance
- Forensic investigations

GFI
NETWORKING
CONTENT SECURITY
MESSAGING

Download your copy today from www.gfi.com/wfl/

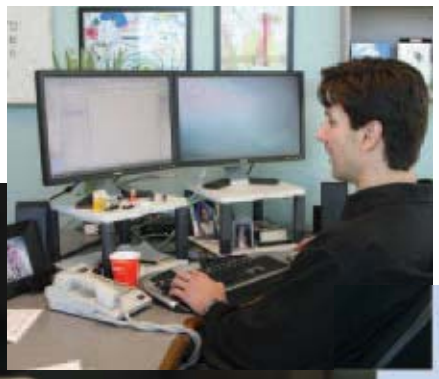
tel: +1 (919) 379 3397 | fax: +1 (919) 379 3402 | email: sales@gfiusa.com | url: www.gfi.com/wfl/

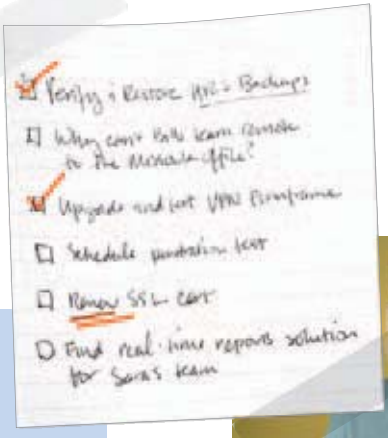


Discover > Explore > Pilot > Deploy > Manage

SPRINGBOARD SERIES

The resource for Windows desktop IT professionals

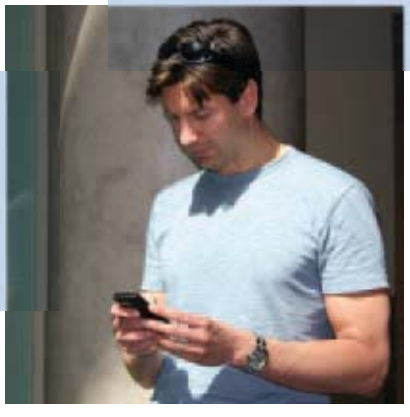






"I don't know" is not an option.
That's why I depend on the Springboard Series.









"My secret: Sometimes *I don't know* the answer.
The Springboard Series makes me look like I do."

www.microsoft.com/springboard

Windows®



Don't despair. EventSentry® has the answers.

Whether you need to get real-time event log alerts, consolidate your logs, ensure that services or processes are running, monitor system performance or track logons, EventSentry® knows what's going on under the hood of your servers and workstations to help you detect and solve problems proactively.

Features:

- Event Log Alerts + Consolidation
- Scheduled Event Log Backups
- Performance & Disk Space Monitoring
- Process & Service Monitoring
- Web Reporting (Open Source)
- Heartbeat Monitoring
- Process, Logon & Print Tracking
- Software & Hardware Inventory
- Syslog Daemon
- Built-in Application Scheduler
- Complete Environment Monitoring
- Log File & File Checksum Monitoring

Notifications:

- SMTP Email, Pager, and RSS
- SNMP (v1 traps) + Syslog (TCP + UDP)
- ODBC Database
 (Microsoft® SQL Server®, MySQL®, Oracle®)
- Text File (ASCII, HTML, CSV)
- Network, Custom Batch Scripts
- Instant Messaging (Jabber)
- Service Control + Server Restart

EventSentry® is backed by excellent and hypersonic support!
Free version available!



Download your fully functional, free 30-day trial now from:
www.eventsentry.com

EVENT SENTRY

© Copyright 2008 NETIKUS.NET ltd. All Rights Reserved. EventSentry is a registered trademark of NETIKUS.NET ltd in the United States and/or other countries. All other trademarks are the property of their respective owners.

netikus.net 1-877-NETIKUS or 1-877-638-4587

TOOL TIME

windowsitpro.com

SYDI Makes Documenting Servers Simple



When I asked my friends on the Mark Minasi Reader Forum for some ideas on cool free tools, Claus Nielsen was one of the first to email me. He wrote, "We needed to document our servers, but it seemed like a daunting task to begin from scratch. Luckily I heard of the SYDI project. SYDI was able to remotely gather 90 percent of the information we needed from our servers. So instead of spending two weeks documenting servers, we spent two days."

I decided to try SYDI-Server, the SYDI version for documenting Windows computers. (There are also versions for documenting Microsoft Exchange, Microsoft SQL Server, and Linux systems.) Getting SYDI-Server was easy. You just go to sydiproject.com and click the Download link. Figuring out how to use it took me a bit longer. Although the default run command is shown next to the download button, I first wanted to read about my options. I eventually found a blog post where the tool's author explains those options (click How-To on the home page, then select *How to Document Servers with SYDI*), which include being able to use it on local and remote machines and to export output to an XML file.

Deciding to run SYDI-Server in the default mode on the local machine, I typed

```
cscript.exe sydi-server.vbs
```

at a command prompt and pressed Enter. SYDI took off. A few minutes later, Microsoft Word displayed a beautiful 35-page report showing me documentation such as the server's name, IP addresses, installed software, and security patches. The list seemed to go on forever.

After just a few minutes with this free tool, I could easily see why Claus was able to document all his servers in just two days. Great find, Claus!

—Eric B. Rux, senior Windows administrator and cofounder of WHSHelp.com

InstantDoc ID 100305

SYDI SFU

READER TO READER

Do More with For

Windows Services for UNIX (SFU) includes UNIX and Linux binaries that you can run from a Windows command line or in a batch file. Installing SFU is easy, and you get a host of new commands that don't exist in Windows. When you combine the SFU commands with the Windows For command, you can create powerful tools.

I found this out firsthand recently. I wanted to email myself the log file from each nightly NTBackup job so I could check it. Because the log files' names are the dates on which the backups ran, I knew that I could use the command

```
Dir *.log /o:-d
```

in the C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows NT\NTBackup\Data directory to get a list of the log files' pathnames, sorted with the newest log file first. However, I needed to extract the filename from the most recent log file's pathname. The Windows For command can't do that on its own. What I needed was a command to read the Dir command's output, find the line containing the current date, and extract the filename so that the file could be emailed to me.

I initially thought of using the SFU grep command to extract the filename. Like the Windows Find command, the SFU grep command finds lines in a text file containing a specified string. However, there's an even better tool: the SFU find command. You can use the SFU find command to find files that meet certain criteria, then perform operations on those files.

Using the SFU find command and the Windows For command, I came up with the command sequence

```
For /f "usebackq" %%T in
  (`c:\SFU\common\find . -ctime 0
  -name "*.log"`) Do Set fn=%%T
```

(Although the command appears on several lines here, you'd enter it on one line in a batch file.) Since you might not be familiar with the SFU find command, let's walk through it. To use the SFU find command from a Windows batch file, you first need to call the command by specifying its pathname. If you install SFU in the default location, the SFU commands are in two directories: C:\SFU\common and C:\SFU\bin. The files in the *common* directory have an .exe extension, whereas the files in the *bin* directory don't. For Windows, you use the files in the *common* directory.

The SFU find command, which is case sensitive like all the SFU commands, can take up to three parameters. The first parameter specifies the location to search. In this case, I wanted to search the current directory and its subdirectories, so I specified a period. The second parameter provides the criteria the files must meet to be included in the result set. In my case, I had two criteria:

- The files' last modification date needed to be the current date. I used the -ctime option followed by a 0 to specify that I wanted to find files in which the last status change was 0 days ago.
- The files' extensions had to be .log. I used the -name option followed by "*.log" to indicate that I wanted only log files. The quotes are necessary to stop the pre-expansion of the * wildcard by the Windows command shell.

The SFU find command has an optional third parameter, which you use to specify the operation to perform on the files that meet the criteria. In my case, I didn't include

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com.

If we print your submission, you'll get $100.

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the InstantDoc ID text box.

this parameter. Note that there are many parameters and options you can use with the SFU find command. Unfortunately, this command's online documentation isn't as helpful as it could be, but you can find a good overview of this command at linuxmanpages.com/man1/find.1.php.

There are some items in the Windows For command portion of the command sequence that are worth pointing out. First, note the use of the usebackq option with the /f parameter. When you use this option, the Windows command shell interprets any text enclosed in back ticks (`) as commands to execute, which in turn allows quotes inside the command.

Also note the double percent signs (%%). When you use an iterative variable (in this case, %%T) in a Windows For command that you execute in a batch file, you need to use a double percent sign. The %%T variable stores the filename that the SFU find command returns. This filename is then set to the fn variable. In the batch file I created, I use Blat and the filename in the fn variable to email the file to myself. (Blat is a free command-line email program at www.blat.net.)

I also used the SFU find and Windows For commands together to solve a similar problem. I wanted to create a batch file that not only sent daily database backup files to an offsite ftp server for storage but also emailed the results of this operation to me so I'd know whether it was successful. To email those daily results, I needed a command to get the current date and extract portions of that date. Using the SFU find command and the Windows For command, I came up with the command sequence

```
For /f "usebackq tokens=1,2,3" %%T
  in (`c:\SFU\common\date
  +"%%A %%m%%d %%d/%%m/%%Y"`)
  Do Set dow=%%T & Set dom=%%U
  & Set today=%%V
```

(Although the command appears on several lines here, you'd enter it on one line in a batch file.)

As you can see, this command sequence uses the SFU date command. You can use this command to obtain the current time in a given format or set the system date. In this case, I use it to obtain the current time. The + sign after the command pathname signals the start of a formatting string that specifies the parts of the date to be returned by the SFU date command and how those parts should be formatted. Each format option begins with a % sign (%% in a batch file). If you specify two options with no space between them, the Windows For command treats the output from the two options as one string. If you separate the two options with a space, the Windows For command treats the output from each option as a separate string, which enables you to assign them to separate variables. In this case, the SFU date command returns three separate strings:

- The %%A option tells SFU to return the full weekday name (e.g., Sunday). The Windows For command assigns this string to the *dow* variable.
- The %%m%%d option tells SFU to return the month and day of the month in the format mmdd. This string is assigned to the *dom* variable.
- The %%d/%%m/%%Y option tells SFU to return full date in the British format dd/mm/yyyy. This string is assigned to the *today* variable.

These format options are only a few of the many options available. You can see all the options by typing

```
date -help
```

in SFU.

In the Windows For command portion of the command sequence, note the *tokens=1,2,3* option with the /f parameter. This option tells the Windows command processor to retrieve the first three strings (i.e., tokens) returned by the SFU date command. The command processor assumes you're using a space or tab as the delimiter. If you want to use another character (e.g., a comma) as a delimiter, you need to include the delims= option with the /f parameter.

The batch file in which I used the second command sequence contains another example of how to use the SFU find and Windows For commands together. You can download that batch file by going to www.windowsitpro.com, entering 100294 in the InstantDoc ID box, clicking Go, then clicking the *Download the Code Here* button.

I hope these examples give you food for thought about using SFU commands with Windows commands. You can download SFU at technet.microsoft.com/en-us/interopmigration/bb380242.aspx. (You can also get the UNIX and Linux binaries at Cygwin—www.cygwin.com.) Before you install SFU, you need to create two files—passwd and group—and place them in the \%SystemRoot%\System32\drivers\etc folder. You don't need to populate these files because you aren't fully using SFU; you're using only the UNIX and Linux binaries. For more information on how to install SFU, see the Windows Services for UNIX web page at technet.microsoft.com/en-us/interopmigration/bb380242.aspx.

—Chris Elvidge

InstantDoc ID 100294

Statement of Ownership

Statement of Ownership, Management, and Circulation for *Windows IT Pro* Magazine as required by 39 U.S.C. 3685; *Windows IT Pro* Magazine, publication no. 1552-3136, filed October 1, 2008, to publish twelve monthly issues each year for an annual subscription price of $49.95. The mailing address of the office of publication, the headquarters of general business of Kim Paulsen, Group Publisher, and Karen Forster, Editorial and Strategy Director, is 221 E. 29th St., Loveland, CO 80538. The owner is Penton Media Inc., 249 W. 17th St., 4th Floor, New York, NY 10011-5390. Penton Business Media Holdings, Inc., of 249 W. 17th St., 4th Floor, New York, NY 10011-5390 owns 100% stock in Penton Media, Inc. The average number of copies of each issue published during the twelve months preceding the filing date include: total number of copies (97,622); paid mail subscriptions (57,339); sales through dealers and carriers, street vendors, and counter sales and other non-USPS paid distribution (9,477); paid distribution through other classes of USPS mail (410); total paid circulation (67,226); free or nominal rate distribution by mail (23,671); free or nominal rate distribution outside the mail (3,957); total distribution (94,856); copies not distributed (2,766) for a total of (97,622) copies. The actual number of copies of single issues published nearest to the filing date include: total number of copies (103,586); paid mail subscriptions (59,725); sales through dealers and carriers, street vendors, and counter sales and other non-USPS paid distribution (8,544); paid distribution through other classes of USPS mail (406); total paid circulation (68,675); free or nominal rate distribution by mail (22,919); free or nominal rate distribution outside the mail (9,138) total distribution (100,732); copies not distributed (2,854) for a total of (103,586) copies.

I certify that the statements made by me above are correct and complete:

—Kim Paulsen, Group Publisher.

SBS 2008 and EBS 2008

Build on Knowledge Every IT Shop Needs

Microsoft's research on SMB IT pays off for networks of all sizes

by Karen Forster

You deploy servers. You know how time-consuming and complex deployment is. And Microsoft knows you know it: To determine what features to include in their new releases, the product teams that developed Windows Small Business Server (SBS) 2008 and the new Windows Essential Business Server (EBS) 2008 thoroughly researched market needs. In the course of that research, the teams performed an experiment to measure just how much time and effort deployment involves. According to Björn Levidow, principal lead program manager for EBS, "We hired somebody to set up Exchange Server and Windows Server 2003, configure IIS, and set up Threat Management Gateway and make it all work nicely. It took that person about 80 hours to get it working correctly."

That experiment led to the streamlined deployment and setup that Microsoft built into SBS 2008 and EBS 2008. But it also led to the identification of problems that affect all IT shops and to the distillation of some best practices to help correct and prevent trouble. Whether you're in a small-to-midsized business (SMB) or a large enterprise, the lessons learned from SBS and EBS research can make a difference to the proper functioning of your network—and your Active Directory (AD) infrastructure in particular.

Top 10 Problems

Microsoft developers found that they could streamline EBS and SBS deployment by finding problems IT generalists didn't realize they had. Björn said deployment "took an expert 80 hours, and required following all the manuals. [The expert] had all the background knowledge ahead of time. But midmarket IT generalists don't have all that background." So, Björn continued, the product developers "set ourselves a goal that we had to make it so customers could install EBS over a weekend."

By testing installations on existing networks, Microsoft discovered common infrastructure problems. Björn said, "The biggest challenge, which we found through our TAP [Technical Adoption Program] deployments, was their existing infrastructure [wasn't] ready to accept an EBS environment configured to best practices. Many of our TAPs had environments that were so dirty that our installs would fail because AD wasn't available. Everything would work fine, but once we started trying to do things that were timing-sensitive or when we had multiple operations right after each other putting some load on their AD network, we'd start getting failures or long timeouts."

The solution to these problems was to create a deployment diagnostic tool for EBS and for SBS. Björn explained, "We built this preparation tool, which looks at their whole environment. The way we learned what to check for is that Microsoft's support services had this great internal tool they would parachute into enterprises, run it, and then take it away with them because it was unsupportable. We took all that knowledge and put it into supportable code. Microsoft support had about 300 different checks. The EBS developers took the 90 checks that were applicable to midmarket companies and coded them in. Now we can run them ahead of time to make sure the environment is clean."

The 90 checks that the EBS and SBS research led to apply not only to SMB IT environments, but to organizations of all sizes. You can download the entire Windows Essential Business Server Preparation and Planning Wizards from Microsoft's website at go.microsoft.com/fwlink/?LinkID=120587. Table 1 shows the top 10 problems the EBS product team uncovered and a link for help on Microsoft's website.

Leveraging AD

Many of the problems uncovered by the EBS and SBS research are related to AD. Microsoft representatives discussed ways they could address these problems in their product development. Kent Compton, a senior product planner for EBS, explained, "Our [customers] know AD. The funny thing is when we ask how many OUs [organizational units] or GPOs [Group Policy Objects] do you have, they don't know. Windows XP, Windows Vista, Windows Server 2003 and 2008 have a total of about 3,000 GPOs. The average midmarket company probably uses about three. They don't do simple things like locking a screen saver so somebody can't come up and fiddle about. The problem with AD and Group Policy is people don't leverage them."

The EBS and SBS teams built tools to help customers take advantage of these technologies. Björn said, "We set up Group Policies for automatic folder redirection every time you create a user. We also set default software update policies for all clients so they're secure by default—also through Group Policy. We are using AD in a much richer way than people in the midmarket might without our assistance of setting up the best practices."

Sean Daniel, a senior program manager for SBS, added, "For Group Policy or the AD technologies, we give customers simple, familiar property pages or wizards in the shell to walk through how to set those things up—if they aren't set up by default—or to tweak them."

"We do the same in EBS," Björn noted. "The [EBS] wizards have a little more flexibility in terms of parameters you can set. The defaults are easier to change because midmarket IT generalists like to have that bit of control more than the SBS customer."

Moving AD and Group Policy complexity into wizards could cause difficulty for administrators when they need to troubleshoot problems. Björn replied, "We designed the EBS admin console with troubleshooting in mind. We have contextual fall-through: We allow you to fall through to various troubleshooting tools, including SCE [System Center Essentials], from our console. SCE takes alerts and events from various places and brings the data up into our console so you can get a single view. We do the same for all the other tools as well. We're the jumping off point, the one place where you can see your whole environment."

Ease for All?

Because many problems identified for SMB IT apply to organizations of all sizes, why doesn't Microsoft just make Windows Server itself easier to use? The answer lies in the greater complexity of IT in large companies. Generalizing the requirements of an SMB is far easier than finding a configuration that would work for more than one enterprise. As Björn said, "Given the size of the company [EBS is] going into, we can assume a bunch of things about how things will be configured by having the three servers. In an enterprise, you can't make those assumptions. So it's not just a matter of simplifying Windows Server. You have to understand enough about the environment and have enough constraints so you can make smart choices in how to simplify it—yet give the customer the tailored functionality for that market segment."

But even if Microsoft can't guess every company's needs, the lessons the product teams have learned from studying SMBs can provide benefits to any company. Check your network for the top problems Microsoft identified, and maybe you'll save yourself headaches. Simplifying configurations and following best practices can pay off for organizations of any size. As Devesh Satyavolu, a product manager for the Windows Essential Server Solutions family, put it, "The real pain in the midmarket is getting to best practice configuration and helping make sure we're simplifying IT. Once they have the best practice IT, it's the gift that keeps giving."

InstantDoc ID 100259



Karen Forster
(karen.forster@penton.com) is the IT Group editorial and strategy director for *Windows IT Pro*, *SQL Server Magazine*, and *System i NEWS* and former director of Windows Server User Assistance at Microsoft.

Table 1: Top Ten Problems Identified in Midmarket Networks

Problem	Explanation	Help Link
Insufficient space in SYSVOL for successful EBS setup	The volume that contains the SYSVOL partition on the {0} domain controller (DC) has less than {1} MB of free space.	support.microsoft.com/kb/222019
SYSVOL Staging Space >80% utilized and could cause AD replication failures	The SYSVOL staging area on the {0} DC is at least 80% full.	support.microsoft.com/kb/222019
A subnet detected in the environment isn't defined in AD	A subnet was not defined in this wizard for the {1} subnet found in the {0} AD site.	go.microsoft.com/fwlink/?LinkId=124336
Flexible Single-Master Operation (FSMO) roles are held by DCs that are distributed across multiple AD sites	The {1} role is owned by the {0} DC that is located in the {2} AD site, which is not a local AD site.	support.microsoft.com/kb/255690
Conflicting IP address subnet definitions	Conflicting subnet definitions between the IP address of 1 or more DCs and the AD site in which that DC is located.	go.microsoft.com/fwlink/?LinkId=124336
The internal/external network adaptor binding order is incorrect	The {0} server has the {2} external network adapter bound before the {1} (MAC: {3}) internal network adapter.	support.microsoft.com/kb/269155
Dynamic DNS registration isn't configured correctly for one or more DNS servers in the environment	Dynamic DNS registration was not recorded for the {1} network adapter on the {0} server.	support.microsoft.com/kb/816592
WMI service on a server in the environment doesn't respond	The {0} server could not be accessed using WMI. Actions that you can perform to resolve this issue might include stopping the firewall before you run the wizard, ensuring that the server is available, installing WMI provider on a Windows 2000 server, enabling WMI access on the server, or removing the server object from Active Directory Sites and Services if the server has been decommissioned.	support.microsoft.com/kb/216364
One or more DNS servers defined in AD aren't responding to queries	The name for the {0} server did not resolve correctly.	support.microsoft.com/kb/291382
The time service isn't running on one or more DCs in the environment	The time service is not running on the {0} DC.	technet.microsoft.com/en-us/library/cc736564.aspx

SBS 2008 and EBS 2008:
The View from the Trenches

by Karen Forster



MVPs Susan Bradley and Nick Whittome get real about the new versions



The Microsoft product teams responsible for developing Windows Essential Business Server (EBS) 2008 and Windows Small Business Server (SBS) 2008 proudly emphasize how much research they performed to ensure that the products met customer needs. To balance Microsoft's perspective, *Windows IT Pro* asked two respected SBS MVPs, Susan Bradley and Nick Whittome, to candidly discuss the products from the community perspective. Has Microsoft's research paid off for the people who will be deploying SBS and EBS? Here's how Susan and Nick see the new launches.

Start with the Essential

As an SBS MVP, Susan looks at EBS as an extension of SBS and even hearkens back to the product that was the ancestor of both: "Anyone old enough to remember Microsoft BackOffice Server in the Windows NT 4.0 era will likely think of EBS as BackOffice's fully developed descendent. The goal of EBS is to bring to the midmarket what SBS has brought to small businesses."

However, Susan is quick to note, "EBS is not just SBS expanded to incorporate three, or potentially four, servers." The architecture of EBS breaks down a network into IT roles. Reflecting this structure, "EBS 2008 Standard edition encompasses three server roles (Management Server, Messaging Server, Security Server), and EBS 2008 Premium adds a Database Server role."

Susan describes each EBS server role, starting with the Management Server: "This server needs to be 64-bit, and Microsoft recommends a minimum of 4GB of RAM. Windows Server 2008 and Microsoft System Center Essentials (SCE) 2007 reside on this first server, which is also the primary domain controller for the EBS network. The SCE role on this server also provides management, monitoring, and patch deployment for the network. SCE lets you set up alerts and scans to monitor the network."

The Management Server is crucial for preparing your EBS rollout. As Susan explained, "When you deploy the three EBS boxes, this is the server that starts the process and provides the guidance for setting up the remaining servers. Like SBS 2008, EBS includes tools for migrating from an existing platform such as an older version of Windows Server. These tools assess the condition of your current system, examining such aspects as your Active Directory (AD) infrastructure. EBS tools also assist in extending your schema to prepare for migration. After you've completed the preparation through the tools, you begin the process of moving your network to three servers with the distinct roles."

Susan has found the migration assistance valuable: "These tools are an excellent feature for both the network administrator and consultants. You can run these planning tools on your existing AD or non-AD environment and improve the ability to successfully migrate to an EBS-based network." (For Microsoft's explanation of these tools and the top issues associated with them, see "SBS 2008 and EBS 2008 Build on Knowledge Every IT Shop Needs," page 27.)

Moving on to the Messaging Server, Susan says, "Email is a key feature of EBS, and the second server houses Exchange Server 2007. This server—which is also a second domain controller for the network, for redundancy—will be your largest server of the three in hardware and RAM requirements. Plan accordingly for this box. Although the minimum memory requirement is 4GB, use the normal Exchange 2007 scaling guidance, and calculate your needs based on the number of users connecting to it and using its services. EBS also includes a one-year subscription to Microsoft Forefront Security for Exchange Server."

The Security Server's role is to protect "the edge of the network. In addition to serving the Edge Transport role of Exchange 2007, it includes Microsoft Forefront Threat Management Gateway, which is the successor to Microsoft ISA Server." Susan continued, "The Security server requires the least processing horsepower of EBS's three servers, but it still needs a 64-bit server with at least 2GB of RAM. I've not seen it get taxed when adhering to that requirement."

For companies that require database support, EBS also has a Database Server role. Susan explained, "If you opt for EBS Premium, you'll receive an additional copy of Windows Server 2008 Standard plus Microsoft SQL Server 2008 Standard edition."

These roles provide the basic IT infrastructure for a midsized business. However, Susan noted a gap: "With all the roles and servers that I listed, you might be surprised to find one missing. I know I did during the beta testing. The role I wanted from the initial deployment was Windows SharePoint Services (WSS) 3.0. EBS will, however, include a console add-on that lets you manage WSS like the other server roles. You can install SharePoint on the Management Server, but it's recommended to place it on a separate server. Microsoft supports WSS 3.0 as an additional server, as long as you purchase the necessary separate licenses."

EBS: The Good and the Bad

Susan approves of the wizard-based deployment model that EBS inherited from SBS—and the EBS model gives administrators more flexibility and choices than the SBS wizards. Plus, the inclusion of planning aids "ensures that when you migrate from an existing network, you can ensure that AD is in a healthy condition." In addi-


Windows Server 2008
HYPER-V
PURE CONSOLIDATED
ENERGY
FOR YOUR SERVER
IT 24-7

toughest



Your potential. Our passion.®

Microsoft®

WINDOWS SERVER 2008 WITH HYPER-V.

The power to wrangle, rope, and virtualize the workloads.

Like most IT, you've got whole herds of servers that need virtualizing. But you don't need some premium-priced solution to rope 'em in. Get Windows Server® 2008 with the virtualizing power of Hyper-V.™ In one solution, you get the power to virtualize, to integrate with a broad range of management tools, and 24/7 availability—all for a refreshingly low TCO. Drink in the details at **ServerUnleashed.com**

Windows Server® 2008

tion, Susan applauds the fact that "hardware manufacturers such as HP are already offering blade server solutions specifically for EBS deployment."

A technology that will likely prove very popular is the Remote Web Workplace portal, which EBS has adopted from SBS. Susan explains, "This website allows secure remote access to Windows Vista and Windows XP workstations. Microsoft supports the separate purchase of Terminal Server licenses, which you can deploy on an additional server. You can also deploy Terminal Services Remote Applications."

On the less positive side, Susan points out that EBS "includes Forefront Threat Management Gateway in the Security Server role. Because you can't and shouldn't move Exchange 2007's Edge Transport server role from this server, you'll seriously hinder your messaging deployment if you decide not to deploy the Security Server role. So if you want to maintain your existing firewall, make sure you place it in front of the Security Server role. Then you can continue to use your firewall solution as it stands today. Some would argue that this setup adds complexity while others argue that it adds an additional layer of protection in front of the server."

In summary, Susan predicts that "the biggest hurdle will be the hardware investment that EBS requires. In many midsized organizations, purchasing three or four servers at one time might not be feasible."

On to SBS

Because Susan and Nick are SBS MVPs, they have strong opinions about SBS 2008. Will they replace existing SBS implementations when the new version is available? Susan said, "SBS 2008 is driven by Exchange 2007's need for 64-bit horsepower, so I'll upgrade when I need to replace hardware. I anticipate that to be in 2009." Nick agreed that the need for 64-bit hardware would delay his deployment of SBS 2008.

What's the key selling point in SBS 2008? Susan likes the fact that "SBS 2008 Premium comes with a second Server 2008 license (32- or 64-bit) and will ship with both SQL Server 2008 and SQL Server 2005 (32- or 64-bit). I like the idea that I can pull SQL Server off the main box and move it to the second server. I can make that second server my line-of-business application box, my SQL Server box, or even a secondary domain controller. Also, the ability to add Terminal Server remote apps to the Remote Web Workplace Console will be great."

Nick likes "the ease of deploying Exchange 2007 with SBS 2008. The wizards do everything for you, and if you've gone through the hell of configuring Exchange 2007 certificates and Outlook Anywhere, you'll really appreciate SBS 2008's excellent automation of this process. As part of this same web wizard, you can perform complicated tasks, such as registering domains, getting connected, and deploying a smart website, in just a few minutes."

What's the biggest advantage in deploying SBS 2008? Susan sees benefits for "a firm that's investing in Vista. The Server Message Block 2.0 TCP/IP stack makes a difference. You'll see speed increases that you don't see in an SBS 2003–based network. Also, several new networking wizards make it a breeze to set up full SMTP email and perform domain integration with a Microsoft Office Live Workspace website and shared space. The wizard of all wizards is called Fix My Network. It reviews DHCP and DNS settings and rectifies problems accordingly. In addition, new POP3 connectors pull email every five minutes, and a wizard helps you set up a smart-host connection for Exchange. These tools are great if you want to maintain legacy email setups."

SBS 2008 isn't without some drawbacks. Susan says she is "most disappointed in the new SBS 2008 monitoring reports because they look terrible in a non-Outlook mail client. You can set up custom reports, but I wish it performed better monitoring of the health and status of my workstations than it currently does. It only looks at the antivirus, antispyware, and patch status of workstations, and keeps an eye on the drive space. I would prefer additional alerts, such as for problems that are predictors of hard drive failures, and I've built some custom alerts to share with the community at www.codeplex.com/sbs."

Nick adds, "Susan is being polite here. The monitoring is just plain awful. We'll have to use third-party products to get a good overview of the desktops on our networks, or find solutions from open-source communities such as CodePlex."

Migration Hurdles

No doubt there are other changes that some will love and some hate. Susan complains that there "is no support for tape backup. The reason is that Server 2008 doesn't support tape as a backup medium, so SBS has also dropped it. Also, people who already have virus protection subscriptions won't like the inclusion of trial versions of Forefront antivirus to protect Exchange and Windows Live OneCare to protect the server. The good news is that you can delete these during the installation process and install your own antivirus solutions."

The biggest disappointment for Nick "is the huge increase in price for SBS 2008. In my opinion, this is a push to get customers to sign up for Software Assurance, which really isn't where the majority of small businesses want to be. SBS 2008 Standard is now $1,089—a huge increase from SBS 2003, which was $599. Although the CAL price appears cheaper with SBS 2008, I see this as a false perception because the CAL price increased between SBS 2000 and SBS 2003. However, I like the fact that you now have the option of purchasing single SBS 2008 CALs." For Microsoft's response to this point, see the web-exclusive sidebar, "Microsoft's Take on SBS 2008 Pricing," www.windowsitpro.com, InstantDoc ID 100271.

Susan believes the upgrade and migration process "will probably be the biggest hurdle for SBS 2008. Because Exchange 2007 requires 64-bit hardware, you can't upgrade in place from SBS 2003 to SBS 2008. You need a unique answer file process to enable the migration wizard, which is a combination of automated tasks and step-by-step instructions to guide you."

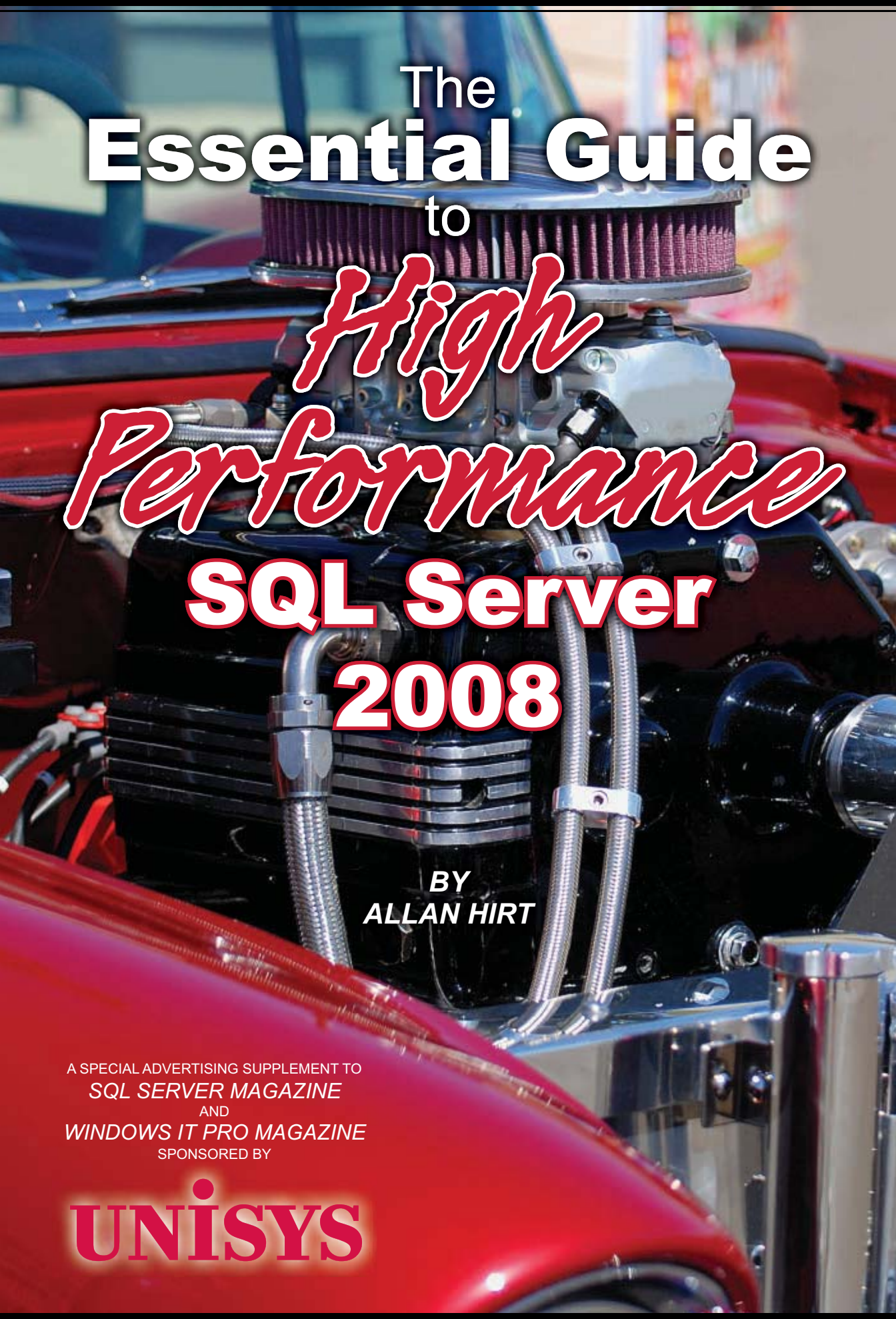
Nick adds: "The migration process is certainly better than in previous versions. The product is well documented, and the wizards are pretty intuitive. WSS migration is lacking and requires that you install the new version side by side with the old. Several consultants have already suggested better alternatives for migration."

Some Improvement, Some Holes

Judging by Susan's and Nick's experience with EBS and SBS, the Microsoft developers got a lot right. But these MVPs also found areas for improvement. If you're considering EBS or SBS, let us know what you think and tell us your views and experiences with the products.

InstantDoc ID 100277

—Karen Forster



The Essential Guide to High Performance SQL Server 2008

BY
ALLAN HIRT

A SPECIAL ADVERTISING SUPPLEMENT TO
SQL SERVER MAGAZINE
AND
WINDOWS IT PRO MAGAZINE
SPONSORED BY

UNISYS



the migration to SQL Server 2008 begins, the inevitable question will be asked in many environments: when we deploy SQL Server 2008, how can we ensure it is highly performing? This guide will address the factors and challenges involved with implementing high performance SQL Server 2008 instances and databases.

How to Size Servers

It must be stated up front that the way to scale SQL Server is up, not out. This has been a sore point for many IT shops accustomed to products where it is easy just to throw another server at the problem. That does not really solve any issues: it is often a patch for an underlying problem that is ignored. You can scale out with SQL Server, but it takes planning when the application is developed. All methods described in this guide are related to scale up. The three main components related to server sizing are obvious from a workload and performance standpoint: processor, memory, and disk. When considering your workloads, keep in mind if you are going to be doing OLTP, OLAP, or DSS. Each has its own signature.

The most crucial factor for the performance of any SQL Server deployment is the disk subsystem since disk I/O is often slower than accessing memory or processor. Storage is usually centralized in many IT environments, giving administrators and DBAs little control over its configuration. Choosing what type of RAID may not be an option, so knowing how the storage is configured and working well with the group who owns and administers the storage is crucial. While one should never place heavily used data and log on the same disks. This is easier said than done, because in the central storage model of the IT world, even if those files are placed on two disks presented to a server, on the backend, the underlying storage of those disks may actually be sitting right next to each other. Just because it is on a SAN does not mean it will necessarily be highly performing. If you are going to be deploying high performance, mission-critical SQL Server, it is always recommended that a dedicated SAN, or at the very least, total control over the disk configuration at the SAN level is granted to the team deploying the databases. Otherwise, there is a good chance that the disk performance may not meet the needs for the application.

Sizing storage for SQL Server comes in two flavors: throughput (measured in I/Os) and overall storage capacity needs. I/O is more important for performance: without the proper I/O bandwidth with low I/O latency, SQL Server will always perform poorly. I/O is reads and writes, not one or the other. Performance is not only important for data and log, but also tempdb if it is used heavily. When configuring your storage for SQL Server, make sure that you check with the vendor to see if they recommend alignment with DISKPART in Windows and get their offset. If the vendor recommends disk alignment and you do not do it, you will have two physical I/Os for every logical I/O issued from Windows up through Windows Server 2003. Windows Server 2008 accounts for this alignment automatically. Disks used with SQL Server should be formatted with the proper stripe size (usually 64k to match its largest I/O operation – the readahead); never assume a default stripe size is right – check with your Windows administrators before installing SQL Server.

How much storage you need in terms of size is dependent upon many factors, not the least of which is how many years the system will be deployed and regulations which require longer periods of data retention. See the section "Growth" for more information. Designing the storage and file layout is much easier for SQL Server once I/O and storage sizing is solved. Remember to account for storage and performance needed for backups as well. To get better read performance you add more physical disks and to improve write performance, you add additional controller channels. Ensuring the HBA card settings are correct also helps.

Memory is the next most important factor in sizing a server for SQL Server. Objects, users, network connections – each consumes memory in addition to what SQL Server actually uses for processing, transformations, and cache. Cache is the most important aspect because if the data is in memory, it reduces the need to go out to disk to read the information. To see how much memory each object uses, consult the SQL Server Books Online topic "Memory Used by SQL Server Object Specifications". The calculations provided will prove invaluable in helping to size your SQL Server implementations.

Historically, processor is third on the list when it comes to performance bottlenecks in SQL Server. There are plenty of applications that have high CPU utilization, but most hit the wall when it comes to disk and memory way before you worry about slices of CPU. When it comes to sizing how much capacity and numbers of processors you need, remember to factor in any other processes that will be running on that server including utilities like third-party backup compression software which adds to CPU utilization. You can also do much more now with two, four, six, and most likely in the near future, eight cores per

Unisys and Microsoft Deliver *High-Performance Value* to Enterprise Customers



Gary Erickson, Unisys vice president of the Microsoft Global Alliance, talks about the high-value relationship Unisys and Microsoft together offer to customers.

Gary Erickson is vice president of the Microsoft Alliance at Unisys and is responsible for development and execution of the Unisys / Microsoft alliance worldwide business plan across the company. Erickson joined Unisys in 1981, beginning his journey within the company as an account representative for the financial market sector in Anchorage, Alaska. His 27 year tenure at Unisys has included everything from sales representative to vice president of several different Unisys divisions, including his current role with the Microsoft Alliance.

His extensive experience in the information technology industry, specifically his solution development, marketing, product management and sales experience are what allows Erickson to be successful in his strategic alliance role at Unisys. Since taking on the role of vice president of the Microsoft Alliance 10 years ago, Erickson has created and implemented a global engagement model and infrastructure focused on generating market demand for Microsoft-based solutions – a model that was recognized as an alliance best practice by the Association of Strategic Alliance Professionals. Beyond implementing new programs and building strategic partnerships, Erickson also created, recruited, and led a global virtual team generating $1.2B annual partner attached revenue.

Erickson holds a bachelor's degree in business administration from the University of Wisconsin.

How do Unisys and Microsoft work together?

Erickson: The Unisys and Microsoft Solutions Alliance delivers highly secure, scalable solutions that harness the power of people and technology so that our customers can achieve a Real-Time Infrastructure. We help our customers achieve total alignment of their business strategy, process, applications, and infrastructure. Unlike other companies that deliver on isolated technology projects, we help our clients see and understand all the technology influences and interactions that affect their business operations. Our joint solutions address high-priority, high-return customer needs in the areas of:

- Managed services
- Virtualization
- Core infrastructure optimization
- Systems Management and Automation
- High–Performance SQL Server and BI
- Unified Communications
- .Net/SOA
- Collaboration & Enterprise Content Management

Together, we provide our customers with proven industry solutions, the visibility to align business and technology, and dedicated expertise for delivery assurance.

How long have Microsoft and Unisys had an alliance?

Erickson: The history of our alliance began well over 10 years ago. During this time, Unisys and Microsoft accomplished a number of outstanding technology milestones around Windows and SQL Server including:

- Engineering collaboration on Windows Server Datacenter edition….and
- Record setting benchmarks for SQL Server Transaction Processing and SQL Server Analysis Services
- In fact, Unisys provides one of the world's fastest performing database platforms with Windows Server 2008 and SQL Server 2008. Record-setting benchmarks include:
 - SQL Server 2008 Integration Services package load times (1TB in < 30 minutes)
 - Microsoft Dynamics CRM 4.0 sub-second response times with SQL Server 2008

Can you tell me something about Unisys key Microsoft–based solutions?

Erickson: The core of our Microsoft offerings and solutions are based on Windows Server 2008. Unisys relies on Windows Server 2008 to provide a scalable operating system platform for Unisys Enterprise-class servers.

Unisys is leveraging its extensive enterprise server expertise to provide new robust and cost- effective solutions based on Windows Server 2008 virtualization technology for large-scale desktop and Exchange environments. This commitment to Windows Server allows us to continue our technology and services leadership in server consolidation and datacenter rationalization.

Why do you think your alliance with Microsoft works so well?

Erickson: Unisys' ability to deliver innovative and powerful solutions on the Microsoft platform connects the value of IT to our customers' business needs. Our alliance works because we're able to focus on what's important to our customers, get the job done and deliver on results.

For more information about Unisys solutions built on the Microsoft platform, please visit www.unisys.com

processor than you ever could with older, slower single-core systems. Modern applications tend to be designed to scale much better in this symmetrical multiprocessing (SMP) environment. Keep in mind that there is more to performance than cores – you do need to worry about the performance of a single core. More cores does not necessarily mean better performance. Learn about the architecture you are going to be implementing.

The bigger question these days is the following: 32-bit or 64-bit? At this point, assuming you are planning on deploying dedicated SQL Server instances on the intended hardware with no other applications and there are no application constraints (such as 32-bit extended stored procedures that are incompatible with 64-bit), go with the x64 architecture. Older 64-bit processors in some cases were slower in terms of clock speed than their 32-bit counterparts, but the speeds have now caught up. 64-bit will not necessarily double your computing power; its benefits are not a math equation where two times the bits equals two times the performance. The biggest barrier to x64 adoption will be updating the skills and processes of your IT organization since switching means changing nearly everything, including ensuring all drivers and software have a 64-bit version. DBAs wanting to deploy a 64-bit SQL Server 2008 implementation should work with the other departments in their IT organization to make it possible, if 32-bit is still the platform of choice at their company. In addition to updated skills and processes, you will also need to check the availability of the software and utilities for x64 such as anti-virus and monitoring as well as hardware drivers such as the ones for HBA cards. Check with your preferred vendors to see if they have x64 versions for the software and hardware you deploy or will be deploying. The same rules will also apply in a transition to Windows Server 2008 – are your organization's skills and processes updated, and do you have equivalents for your tools for that platform? Windows Server 2008 should be seriously considered for SQL Server 2008 as it will help with increased performance and other aspects of SQL Server such as security.

A big fallacy when it comes to servers – especially in the x64 age – is that you can get away with only blades or smaller 1U servers and achieve the same scale and performance. To some degree that is true, but there is still a need for larger, "big iron" servers depending on your requirements. All servers have a point at which they cannot scale. Will you hit it sooner or later on a blade or 1U? While there are no guarantees, if you purchase hardware with limited capacity for expansion, there will be a hard limit to how far you can go. If you're trying to run your largest, mission-critical system accessed by 10,000 employees that needs to be up 24x7, be in place for five years, and be highly performing that entire time going large is going to offer you much more flexibility and growth than a small server. Part of the reason there is a drive towards consolidation and virtualization is that this SQL Server sprawl with small servers has inundated many IT organizations.

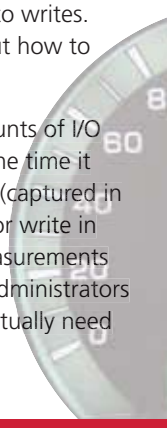
Applications

Applications hold the key to the performance of your databases. If a database server had no applications to connect to it, it would remain highly performing since it would have little demand on processor, disk, or memory. Database servers need to be sized appropriately. The problem is that most database servers are bought well before the application has even been developed. The process is usually something like this:

- A decision is made to deploy an application
- Due to the lead time for ordering and receiving servers, then racking and stacking them (at least a three month process), production servers are ordered with no real information to go on
- The server goes into production and is often either too large or underpowered. Too large is fine from a performance standpoint however it may be seen as wasteful by IT since the server is not utilized "enough". Underpowered means that you are already starting behind the proverbial 8-ball from day one. The goal is to achieve a happy medium.

One of two things needs to happen when you place future server orders. The best method of sizing servers properly is to develop an application, or get a third-party application in and test your workload against it. Even if you test on a smaller server to measure processor, memory, and disk usage, you can extrapolate numbers. Here are some items to collect and measure:

- The overall processor utilization on average.
- The amount of memory and processor used by the SQL Server process – not just the server alone.
- Know how tempdb is being used. Some databases and applications use it heavily, others not. This will affect the disk configuration and ultimate performance of your SQL Server instance.
- Know the ratio in your application of reads to writes. This will not only help determine growth, but how to help measure your I/O performance.
- Physical disk utilization to measure the amounts of I/O being consumed both in terms of size and the time it takes to complete a read or write operation (captured in counters such as the Average disk/sec read or write in Performance Monitor in Windows). The measurements of I/Os will open a dialog with the storage administrators and storage vendors to get you what you actually need



for disk performance. The choice of your backup method will also determine the scale for the log file

- Know what the system looks like at rest (generally measured before the system goes into production), at its busiest (for example, month end close), and what it looks like during normal load. This is especially important if you are re-deploying a SQL Server for an already existing application. You should have performance data going back to the initial day of production to measure growth. If you do not, start now. After deploying SQL Server 2008, you can use the new feature called Data Collector to start capturing and analyzing performance data.

You do not need to measure every performance counter every second of the day on every server. Be smart - it will be virtually impossible to analyze that much data. Only capture what is needed and expand from there as needed.

It should be pointed out that the biggest key to testing an application is to ensure that it is not only tested for features (generally done in singular tests), but under load. Without throwing your actual workload at a system, any sizing is a guess.

Growth

Growth is directly related to usage. The most important thing to account for when sizing servers is how long you plan on having this entire solution in place. No one sets out to buy servers to only be in production for two months; the average lifespan for most servers tends to be three to five years or longer. That means a server purchased in 2008 may be in production until 2013. That is a long time.

Going back to application testing, knowing the signature of that application from the memory and processor standpoint will help. For example, if you measure on a test system that you are already at 35% CPU utilization with 4,000 employees using the application but plan on expanding to 8,000 employees in 12 months, if the CPU load nearly doubles in that timeframe, you will be dangerously close to capacity with four years to go.

When it comes to disk, as applications have become more and more complex, they are utilizing and storing increasing amounts of data. This data is also becoming larger to store with the introduction of unstructured, BLOB, and geospatial data. Since disk is seemingly cheap, application owners are often assuming IT is going to be able to compensate for their storage demands used by a feature. This is a poor assumption. While disk is cheaper, it is not free. There is a finite amount that any storage can scale before needing to buy more disks or hardware. Storage administrators and DBAs need to be in conversations with application owners and developers long before it is deployed; at that point, it is too late.

Another issue related to disk and growth is regulation by government or external entities. Many industries must keep data around longer, whether it is in the main database or keeping backups around for many years. This puts a drain on all IT resources including DBAs since the cost of maintaining that much data gets harder, not easier, as time goes on and windows for performing preventative maintenance such as index rebuilds will consume more time than an outage will allow. IT will suffer under the strain of retention if it is not accounted for up front.

Finally, there is the simple math of disk growth: knowing how big the data and log files will grow in addition to backup storage and its requirements. Every application vendor or owner should be able to tell you the average size of an insert so DBAs can do calculations on size usage. For example, if an application uses 20KB per insert, and there are 1000 inserts an hour that equates to just under 20MB/hour. That equates to about 175GB/year in growth. If that is based on current application usage, not future (which will change over time), you need to figure out as per the example above how adding employees may change this number. Remember that the log file has to account for tasks such as index rebuilds, so as the data usage grows, so will log usage.

When it comes to backups, backups generally grow proportionally to data size. Even if you are using SQL Server 2008 Enterprise Edition's backup compression or one of the third-party vendor backup compression utilities, they will not solve all storage problems. They help, but if you need to store multiple backups on disk – especially with VLDBs – it will be a challenge. Be smart from the start, and you will stay ahead of, not behind, the problem.

Availability

Poor performance often leads to poor availability since queries that take longer, issue table scans (instead of hitting indexes), locks and blocks, and other issues can lead to a



Without throwing your **actual workload** at a system, **any sizing** is a **guess.**

downward spiral to the point of total unavailability of a database or application. If you need to take unplanned downtime to fix a performance issue, that's an outage that contributes to missing availability SLAs. One of the most common areas of reconfiguration is the disk subsystem. Perception is also reality: if end users think that the system is slow, it is often considered an outage since the application may be virtually unusable. Never let a performance issue become an availability problem; this can generally be avoided by proper maintenance and sizing.

It is no longer a 9 to 5 world – servers and systems need to meet the demands of global businesses and customers at any hour of the day. That does not happen easily and takes reliable hardware along with careful planning, deployment, and ongoing, proactive administration. Availability is dependent on formal service level agreements (SLAs) set up between the application units or the business and IT. SLAs extend to performance as well. Formalizing availability and performance SLAs allows both sides to measure and be accountable. Without SLAs, it is impossible to size and deploy systems because there are no formal guidelines to measure against. The SLAs should be continually monitored and revised as needed.

Consolidation

Consolidation is driving a need for SQL Servers that are more highly performing than ever. Most companies have varying numbers of older, out-of-date, inefficient, under- or over-utilized servers that would benefit from consolidating to fewer servers and/or instances of SQL Server. Optimizing a SQL Server environment through consolidation can provide a measurable, long-term benefit not only to the IT organization, but to a business' bottom line. The choices for consolidation are varied: single or multiple instances on a single server or cluster or virtualization with a technology such as Windows Server 2008 with Hyper-V. Your strategy will depend on your needs, but SQL Server supports both approaches. Many times, it may be worth considering one larger server that can either be partitioned into smaller servers or used as one very large, very powerful server that can host many virtual servers with Hyper-V. The acquisition cost may pay for itself over time, and it should be considered a viable option when considering consolidation of SQL Server databases and instances.

Budgets

The final factor for performance is not an obvious one: your budget. The architect may have visions of the ultimate scalable system when designing, but as soon as he or she sees the amount that is allocated, reality smacks them in the face. Very few companies give their IT organization carte blanche when it comes to ordering systems. This is true whether or not you have hundreds of millions of dollars in the bank or just hundreds. Money is tighter everywhere, so ordering the right server for a reasonable price is going to make or break the implementation long term. Making a choice largely based on price is a recipe for disaster. This is often in direct conflict with most organizations. It is not uncommon for an IT shop to have three to five "standard" server builds to choose from, and an implementation has to fit into one of them. It is a bit like trying to put a square peg in a round hole. If you have other needs, you either cannot get it or it takes a lot of jumping through hoops to get there. Deploying servers and other hardware components that are not adequate will cause availability and performance issues sooner rather than later, and the price to fix those problems is often more expensive than if the proper solution had been purchased from the start. Cost cannot be ignored, but spend wisely. Compound cost with preferred hardware vendors where you can only purchase from certain companies as well as be limited by hardware selection, and the drive to over-consolidate or virtualize things does not get easier. The right solution will be a compromise.

Conclusion

Deploying highly performing SQL Server systems is not just a DBA or IT problem. Proper performance begins from day one of any solution or application's planning and requirements – well before implementation or a line of code is written. Often times DBAs are not involved at this phase, but pay the price for it later. DBAs can help by assisting in the process to size, acquire, and deploy servers as well as ensure that the proper proactive maintenance is in place to keep the databases and instances running like well-oiled machines. The best thing you can do now in your current environments if you are not already is to start to define, analyze, monitor, and project what your various workloads are and will be. The more information you have up front, the better the conversations will go with both internal groups as well as with hardware vendors. Then and only then can you implement and deploy appropriately priced and sized servers for SQL Server that meet the performance, availability, and growth needs for the business.

Allan Hirt has been using SQL Server in various guises since 1992. For the past 10 years, he has been consulting, training, developing content, speaking at events, and authoring books, whitepapers, and articles. His most recent major publications include the book *Pro SQL Server 2005 High Availability* (Apress, 2007) and various articles for *SQL Server Magazine*. Before striking out on his own in 2007, he most recently worked for both Microsoft and Avanade, and still continues to work closely with Microsoft on various projects. He can be reached via his Web site at http://www.sqlha.com or at allan@sqlha.com.

Securing Windows Desktops Using Group Policy

Configuring system, application, device, and IE security

by Darren Mar-Elia

Managing Windows desktop security can be complex, with a myriad of tools and approaches available. However, Windows OSs include a built-in tool that has all the capabilities most organizations need to create secure, locked down desktops across any size environment—Group Policy.

Group Policy is often thought of by many IT administrators as a tool for performing desktop management tasks such as deploying software, redirecting folders, or locking a user out of regedit.exe. However, Group Policy is also the primary Windows tool for managing security configurations. In fact, Group Policy includes quite a few security capabilities that you might not be aware of. In this article, I explore some of Group Policy's security features, explain how they work, and give you some tips for getting the most from them.

Core System Security

I break Group Policy's security configuration capabilities into the following general categories: core system security, application and device restrictions, and Microsoft Internet Explorer (IE) security. The policy settings in the core system security category can typically be found in Group Policy Editor under Computer Configuration\Windows Settings\Security Settings, as shown in Web Figure 1 (www.windowsitpro.com, InstantDoc ID 100264) from a Windows Vista system. Here are some of the features found in the core system security area of Group Policy.

Account Policies

You might be familiar with this section of Group Policy because it's where password and account lockout policies are set. For example, you can set a minimum password length or require passwords to contain complex characters in this area of Group Policy. If you define these policies in a Group Policy Object (GPO) linked to the domain (e.g., within the Default Domain policy), the password policy is processed by all the domain controllers (DCs) in your domain and the GPO controls password policy for your domain user accounts. When the password policy is defined in a GPO linked to the domain, it will also be processed by all workstations and member servers in the domain and will set account policy for any local accounts defined on those systems.

As you might know, you can have only one domain password policy defined through Group Policy. However, Windows Server 2008 supports a new set of password policy objects, defined in Active Directory (AD), that give you more granular control of password policy within a single domain.

Local Policies

The three security policy areas under Local Policies let you control a variety of security settings on your Windows systems. For example, these policies let you use Audit Policy to configure which events are collected by the Windows Security event logs on your servers, use User Rights Assignment to configure who can access a particular set of servers or workstations via Remote Desktop, or use Security Options to configure whether the Administrator account is enabled on a given set of systems and renamed something other than Administrator.

Audit Policy is fairly straightforward in that it lets you control which types of events will be collected by the Windows Security event log. You can specify success and/or failure events here for auditing types ranging from AD access to system object (e.g., file and registry key) access. Depending on where a GPO defining auditing events is linked, you can enable auditing on DCs or member servers and workstations. For example, if I link a GPO containing an audit policy that enables directory service access auditing to the Domain Controllers organizational unit, it will be processed by all the DCs in my domain and thus all access to AD will be logged on the DC that serviced the access request.

User Rights Assignment is another powerful security tool within Group Policy. This tool lets you control who can do what on a given system. Examples of user rights include the Logon Locally right, which lets you control who can log on interactively at the console of a server or workstation, and the Load and Unload Device Drivers right, which grants a group or user the ability to install device drivers such as printer and display drivers. By creating a GPO that's linked at the domain level and populating the Deny Log on Locally right with the Authenticated Users group, you would effectively prevent all the users in your AD domain from logging on to their workstations. Obviously, the point of this example isn't to show how to break things, but to show how powerful User Rights Assignment can be and how careful you need to be when using it. As with other policy settings, you want to make sure that the GPO in which you're setting user rights applies only to the computers you intend it to and that the rights you're granting or revoking are granted or removed from the correct user groups.

Another thing to keep in mind about User Rights Assignment is that the list of rights that you see in Group Policy Editor changes depending on which version of Windows you're editing Group Policy from (i.e., the version of Windows that you're running Group Policy Editor on). Newer versions of Windows, such as Server 2008 and Vista, contain more user rights than older versions such as Windows XP. So, if you define a user right in a GPO running on Vista, and that GPO is applied to an XP system that doesn't know anything about that user right, the XP system will process the policy but then ignore it.

You can quickly compare the differences in security settings between versions of Windows by downloading the Group Policy Settings Reference spreadsheets that Microsoft maintains for each version of Windows at download.microsoft.com. Search on the term "Group Policy Settings Reference" to see the spreadsheets for each release. The spreadsheets contain a list of all the default Administrative Templates for that version, as well as security settings.

You can use User Rights Assignment, as well as some of the other security areas in Windows, to configure roles that define who can do what within your environment. The built-in groups, such as Server Operators and Backup Operators, are just groups that have been granted a set of user rights and permissions for other resources on a system. You can certainly create a Desktop Administrators group and grant that group rights to perform whatever tasks are needed on your Windows systems, without having to include members of that group in the Administrators group on every system.

The final area in the Local Policies section of Group Policy Editor is Security Options, which is located under Local Policies\Security Options. I call these settings the "vulnerability controls" because they define security settings that control configuration behaviors related to a system's security posture. For example, within this section, you can configure Server Message Block (SMB) signing requirements on clients or servers. SMB signing is a form of secure communication that makes it difficult for attackers that have access to the network between systems to hijack that traffic. Within this section, you can also control the behavior of Vista's User Account Control (UAC) feature, as shown in Figure 1.

Perhaps the most interesting thing about the Security Options section is that the list of security options that are presented in this section, while dependent on the version of Windows you're running Group Policy Editor from, can be manually changed. The list is configured from an underlying file, called sceregvl.inf, that's contained within the %windir%\inf folder on the machine you're configuring. Within this file, each of the policies that you see in Security Options is defined, and you can edit the file for additional settings that you want to control via Group Policy. More information about customizing this file can be found at support.microsoft.com/kb/214752.

Restricted Groups Policy

The purpose of the Restricted Groups policy is to provide a mechanism for controlling local group membership on member servers and workstations. For example, you can use the Restricted Groups policy to ensure that only Help desk administrators are members of the Remote Desktop Users group on all your workstations. Restricted Groups has two modes of operation—Members and Member Of. The Members mode is the most restrictive mode. It says that for a given local group on a set of workstations, only the listed users and groups are members, and all other groups or users are removed (with the exception of the local Administrator account, which is never affected by the Restricted Groups policy). By contrast, the Members Of mode lets you add users and groups to other groups non-exclusively. In other words, you can create a policy that says *Always make the Desktop Administrators group a member of local Administrators* on any computers that process the policy. In that case, Desktop Administrators is added to the local Administrators group, but no other group members are affected.

The new Group Policy Preferences feature, which is included in Server 2008 but can be installed on XP and later, also includes the ability to control groups within the Computer (and User) Configuration\Preferences\Control Panel Settings\Local Users and Groups policy area. You can use this feature to perform tasks such as rename groups and selectively add or remove specific users and groups from group memberships. Group Policy Preferences provides a much more flexible version of the Restricted Groups policy, and I recommend using it as an alternative if you're a Restricted Groups fan but don't like its limitations.

I just want to say a final word about using Restricted Groups and Group Policy Preferences. You might be tempted to try and use these policies to control AD group membership. However, these types of policies aren't designed to be used in AD's

Learning Path

WINDOWS IT PRO RESOURCES

For more information about using Group Policy:

"Configuring How Often to Update Group Policy Security Settings," InstantDoc ID 97943

"Managing Microsoft Office 2007 with Group Policy," InstantDoc ID 97829

"Group Policy Essentials No Sys Admin Can Live Without," InstantDoc ID 97780

"Troubleshooting a Group Policy Processing Error," InstantDoc ID 97349

For more information about restricting removable storage devices:

"Controlling Removable Storage Access," InstantDoc ID 98017

"Configuring a RAS Policy that Limits the Use of Removable Storage Devices," InstantDoc ID 97874

multimaster environment, and you can get into some ugly scenarios in which Group Policy applies group membership changes at different times from different DCs. This can be a problem because group memberships are replicated from the DC that originates the change. Because Group Policy is processed equally by every DC in a domain, each DC would process identical changes to AD group membership as specified by the Restricted Groups policy, and you would essentially be "ping-ponging" identical replication changes of group memberships across all DCs, depending on when each DC processes the policy.

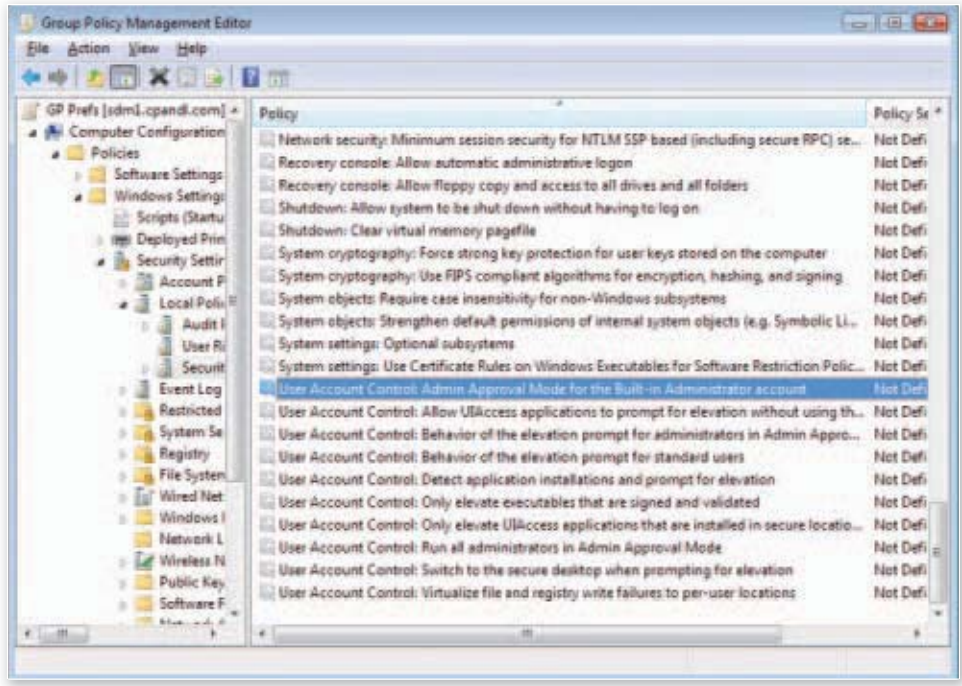


Figure 1: Viewing UAC settings within Security Options

System Services Policy

The System Services policy lets you control which Windows services are started on a given computer. It also lets you control the permissions on a service. For example, you can use this policy area to grant only your server administrators the ability to stop and start the Print Spooler service on all Windows servers acting as print servers. You can use the System Services policy to grant a select group the ability to perform their job without requiring them to be administrators on the systems that they need to access.

Group Policy Preferences, located under Computer Configuration\Preferences\Services, also provides a policy for controlling system services. This feature also provides you with additional control over service configuration, including the ability to change the service account and the service account password on a set of systems. The latter capability is powerful because previously when you had a service running on a bunch of machines in the context of a user account, you had to visit each machine to change the service account password when you wanted to change the user account's password. As a consequence, many organizations avoided changing the service account password, which is a big security risk because many service accounts are more privileged than user accounts. With Group Policy Preferences, you also have a mechanism for pushing that change to all of your computers so that you can change your service account password regularly.

Registry and File System Policies

These policies provide you with the ability to centrally mandate file system and registry key permissions, respectively. For example, say you want to lock down a certain file or folder that exists on all your desktop systems, such as a workstation's HOSTS file, so that malware that gets onto the system can't easily modify that file. In that scenario, the File System policy lets you centrally define permissions and permissions inheritance that should exist on that file on all computers that process the policy. But generally speaking, the file system and registry security policies aren't used very often as a way of centrally managing file system and registry security and can be problematic if misused. These policies aren't designed to work well when repermissioning large trees of files and folders or registry keys. They simply don't perform that well during Group Policy processing and have been known to slow systems to a crawl when a policy is being processed. The problem is exacerbated because security policy automatically refreshes every 16 hours by default, even if no policy changes occur.

If you need to do some file system or registry permission tightening, I recommend using an out-of-band method that doesn't rely on Group Policy, such as scripts, Windows security templates, or third-party security tools. That being said, it is possible to use these policies if you're permissioning only a small number of files, folders, or registry keys, and it can be an ideal way to ensure that these key resources are secured and stay secure, given the recurring processing behavior of Group Policy.

Application Restrictions

In an ideal scenario, you would like to define every process that users can run and exclude all unapproved processes. That way, if users install something on their systems inadvertently, you can ensure that it won't be executed. This is the general premise behind Software Restriction Policies (SRP), which are located under Computer and User Configuration\Windows Settings\Security Settings\Software Restriction Policies. Essentially, you can control, through a variety of rule mechanisms, which code is allowed to run.

SRP can be configured to run in three different modes. The default mode lets all code execute and the administrator restrict those applications or scripts that he or she explicitly wants to deny. This process is called blacklisting, and although it's easy to administer, it's not very secure because

you don't know what you don't know and it's impossible to specify every piece of code that users might run.

The second mode is called whitelisting and is the most secure way to use SRP, but it requires more management on the part of the administrator. In this mode, you can set the default execution level to Disallowed, meaning that no code will execute on the system other than core Windows code and any other applications or scripts that you specify. You can set the default mode under the Security Levels folder within Software Restriction Policies, as shown in Figure 2.

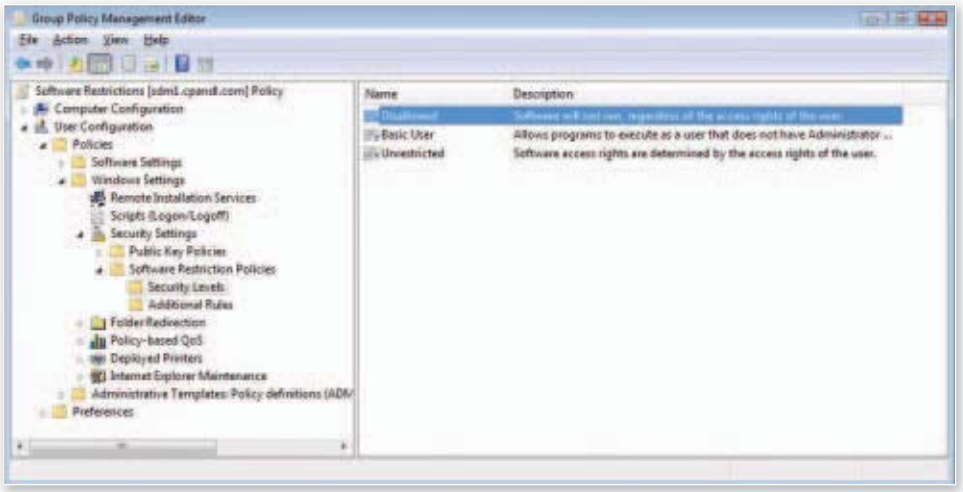


Figure 2: Setting the default software restriction level

When you enable this mode, you must create rules that specify which code is allowed to execute. To do so, you need to know which processes your users will run and keep up with their demands for new applications. Although this can make the process of managing whitelists onerous, it does provide for a very secure environment if your users run only a handful of applications. For example, when you whitelist the applications that are allowed to run, users who inadvertently download malicious code can't run that code because it isn't on the list of approved applications. You define allowed and disallowed applications using the SRP rules that I describe later.

The final mode, called *Basic user*, was first exposed in Vista but is also supported in XP. In scenarios in which your users run as administrators, when you set the default level to *Basic user*, al processes that an administrative user runs are stripped of their administrative tokens, which essentially forces the process to run as a non-administrative user. This approach can be useful if you want to ensure that your administrators aren't running certain processes using their administrative accounts.

The basic approach for using SRP is to first set the default Security Levels to Unrestricted, Disallowed, or *Basic user*. You can then create rules by clicking the Additional Rules folder within Software Restriction Policy, as shown in Web Figure 2. These additional rules provide for exceptions to either enable or disable certain processes' ability to execute. SRP comes with four rule types: hash, path, certificate, and network-zone rules.

- Hash rules—Hash rules are used to uniquely identify an executable piece of code. When you use a hash rule, you pick a particular version of an executable or script and say that only that particular version is Unrestricted or Disallowed. If the user renames the executable, the hash is still valid and the user is blocked, if it's set to Disallowed. However, any time the application changes versions, you'll need to create a new hash rule to reflect that change. If applications have different versions for different Windows releases, each version needs its own hash rule. This type of rule is cumbersome to maintain for lots of applications, but bulletproof for ensuring that a particular application can or can't run. The hash rule is computed by Group Policy Editor at the time that you add the executable to the policy.
- Path rules—Path rules are more flexible than hash rules. They let you specify a path in the file system that contains executable code and allow or disallow all code found in that path (and its child folders as well). You can use wildcards and environmental variables to define path rules, making the rules even more flexible. The downside to path rules is that they're only as good as the permissions on your local file system. If your users can simply copy code they want to run into a different folder to get around a path rule, your path rules won't help much. For example, temporary file locations are typically writeable by users, so you should create a path rule that prevents any code execution from the various temporary file locations in Windows. For this reason, a combination of path rules, hash rules, and tight file system permissions might prove to be the best solution.
- Certificate and network zone rules—These rules are the least frequently used. Certificate rules let you specify code that can run based on who signed the code with public key certificates. The downside to these rules is that they require you to ensure that all code that's run is signed, which isn't always feasible. Network zone rules let you control how files are installed based on where they came from but are almost useless because they apply only to Windows Installer (.msi) files. Also, if a user downloads a setup.exe file, this rule is ignored.

Device Restrictions

Controlling what users do with your valuable business data is equally as important as controlling which code they execute. Protecting your data involves not only good data security where the data is stored, but also being able to control whether your users can physically take the data off their machines. In this era of $20 multigigabyte USB thumb drives, an awful lot of corporate data can just "walk away" without your knowing it. Enter Group Policy–based device restrictions. These device restrictions were made available in Server 2008 and Vista systems under Computer (or User Configuration)\Administrative

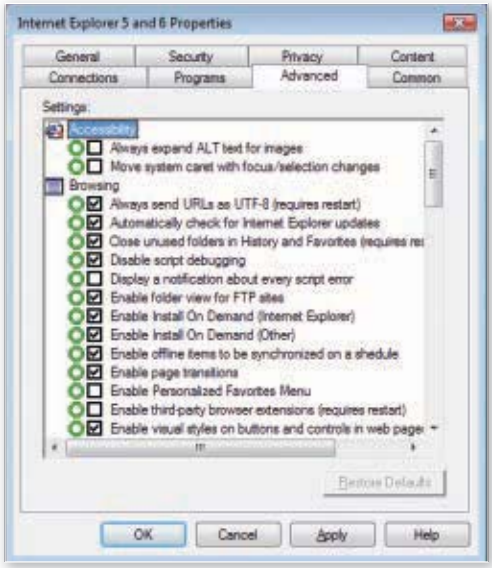


Figure 3: Accessing IE's advanced options using Group Policy Preferences

Templates\System\Removable Storage Access. You can deny read or write access (or both) for any class of removable storage, including USB thumb drives, writeable CDs and DVDs, and removable hard drives, as Web Figure 3 shows.

Previously, if you were in a pre-Vista desktop environment, you were out of luck unless you bought third-party device restriction products. However, with the introduction of Group Policy Preferences, device restrictions are now extended to Windows Server 2003 and XP. You can enable or disable the use of specific device classes by their unique ID under Computer (User) Configuration\Preferences\Control Panel Settings\Devices. Although this feature doesn't provide the same level of granularity as the Vista device restrictions policy we discussed earlier to control the ability to read but not write to a given device type, you can at least create a set of policies that restrict, for example, all removable storage devices, as shown in Web Figure 4.

IE Security

Of all the areas I've discussed, perhaps the most challenging to configure via Group Policy is IE. The reason for this is that there are at least three different ways you can configure IE using Group Policy. The first way to configure IE is by using the IE Maintenance policy (under User Configuration\Windows Settings\IE Maintenance Policy). The second way is by using the Administrative Template policy (under Computer—or User—Configuration\Administrative Templates\Windows Components\Internet Explorer). The third way you can configure IE is by using Group Policy Preferences' features (under User Configuration\Preferences\Control Panel Settings\Internet Settings).

Each of these three areas has its strengths and weaknesses when configuring IE. For example, if you want to configure settings such as IE's proxy or home page, you can use the IE Maintenance policy or Group Policy Preferences to do so. Of the two, I recommend using Group Policy Preferences if you can because the IE Maintenance policy has a long of history of not being very reliable in terms of delivering policy settings to clients. Of course, in most cases, Group Policy Preferences are just that—preferences. They don't prevent users from making changes to, for example, proxy settings, as the IE Maintenance policy does. For that reason, if you use Group Policy Preferences to control something like proxy settings, you'll need to use the Administrative Template policy to disable the page within IE that lets the user access those settings. The goal behind IE security policy is to ensure that users who are browsing websites aren't allowed to access or download malicious content. By using features such as IE proxy enforcement, you guarantee that users get to the Internet through your point of control—the proxy server. By locking down elements of IE within Administrative Template policy, you ensure that the user can't change IE's configuration to get around your restrictions.

If the security configuration task you need to perform is setting IE zone security (which lets you centrally control which websites should be considered safe) or assigning website addresses to popup blocker lists or security zones, you can use all three methods to control these settings. Each method has a different behavior and supports a different set of options. For example, you can use the policies under Computer (or User) Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page to configure security for each IE zone (e.g., Trusted, Intranet, Internet), as well as a site-to-zone assignment list that lets you specify which websites should be added to each security zone for your users. If you use this method, users will be unable to add to or change these settings in IE—they will be totally locked out. However, if you use the IE Maintenance policy, you can configure zone security and site-to-zone assignment, but users will still be able to add websites to a given zone. Finally, if you use Group Policy Preferences, you'll be able to configure zone security but won't be able to assign websites to zones. However, Group Policy Preferences gives you full access to all the settings on the Advanced tab under IE's Properties (shown in Figure 3), which the other two methods don't.

Resources that Can Help You Get Started

Although there are often multiple methods for configuring the same set of items, there are few desktop security tasks that you can't accomplish using Group Policy. For help getting started securing your desktops, I recommend checking out the security guides that Microsoft has made available for Vista and XP. You can download them from download.microsoft.com by searching on the term "Security Guide." These guides include best practices for desktop security configuration, as well as security templates and spreadsheets of settings that define secure configurations. In addition, Microsoft provides the GPO Accelerator (www.microsoft.com/downloads/details.aspx?FamilyID=a46f1dbe-760c-4807-a82f-4f02ae3c97b0), which offers prebuilt GPOs that you can import into your environment and use to implement the best practices specified in the security guides. Although these prebuilt GPOs might not be exactly what you need in your environment, they can give you a starting point to work from as you implement and test secure configurations within your network.

InstantDoc ID 100264



Darren Mar-Elia
(dmarelia@windowsitpro.com) is a contributing editor for *Windows IT Pro* and is CTO and founder of SDM Software (www.sdmsoftware.com). He maintains a Group Policy resource website (www.gpoguy.com) and is coauthor of *Microsoft Windows Group Policy Guide* (Microsoft Press).

10 Reasons to Deploy Windows Vista

With these great features, how can any company resist the switch?

by Mark Minasi

At the tender age of a year and a half, Windows Vista remains the Rodney Dangerfield of Microsoft OSs—it don't get no respect. And that's a shame. Its biggest competitor (no, not Leopard—Windows XP SP3!) is darned good, but a close look will show that Vista is better in many ways. If you're staying with XP because you're satisfied with it, then great, but don't avoid Vista just because your plumber's cousin's stockbroker heard that it was bad. Here are 10 reasons you should consider making the switch.

1. You won't need as many images. If, like most of us, you deploy your desktops with an image-based system such as Symantec Ghost or Microsoft's free ImageX tool, then you know that XP images tend to be hardware-specific: Create "the sales laptop image" on a Toshiba laptop, for instance, and it often won't work well on an HP or Dell laptop. Vista is much more accommodating; you often need only two images for your entire organization: a 32-bit image and a 64-bit image.

2. Finally, a desktop search that works! For nearly 10 years, Windows and Office have included tools that index the files on your computer to make searching for those files possible. Unfortunately, those tools have had a tendency to be clumsy and slow. In contrast, Vista's search index works unobtrusively and makes for lightning-fast searches.

3. A more complete backup tool. Ever tried to rebuild an XP box from scratch, using only a set of files created by XP's built-in backup routines? Ugh. Vista changes all that with its Windows Complete PC Backup and Restore, an image-based backup system that backs up your whole computer to one big file. My experience shows that this system works quickly and allows bare-metal restores to quite dissimilar hardware—just make sure that the target hard disk is the same size or larger than the original.

4. Start great conversations. Next time you're out with your techie friends, tell 'em that you're switching to Vista—there will be plenty to talk about after that! Seriously, if you *are* moving to Vista and people ask you why on Earth you'd do that, remind them that just about every Vista complaint—it's slower than the previous version, there aren't any drivers, it's not backward compatible—is a complaint that people leveled at XP when *it* was new. Look, XP's a great OS, and if you're happy with it, then by all means stay with it—but don't bypass Vista because of second-hand FUD.

5. Windows BitLocker Drive Encryption protects your mobile data. Laptops are great for busy travelers . . . until they're accidentally left in a bar, on a plane, or in a cab, as reportedly happened to hundreds of thousands of systems last year in the United States. In contrast, absentminded folks who exploit BitLocker's encryption system might still lose their laptops, but no one will get their data. BitLocker is available on Vista Ultimate and Enterprise (although, incomprehensibly, not on Vista Business).

6. Get more out of Group Policy. Vista includes about 700 new Group Policy settings that let you control fleets of computers from one central location. Some new options include controlling power management settings, allowing nonadministrative users to load approved drivers, and restricting which devices users can install on a Vista box.

7. Get a tougher Windows. Service programs wield great power in Windows, making them irresistible targets for malware writers: seize a Windows service, and you've often seized Windows itself. Vista uses a more secure way of building Windows services so that they have less potential to do damage and are isolated in their own little private universes, which makes a compromised service a much less juicy prize.

8. Confuse the bad guys with ASLR. Another Windows toughener is Address Space Layout Randomization (ASLR), a feature that rearranges the relative locations of Vista's different components in memory. Past creators of Windows worms such as Code Red, Nimda, SQL Slammer, and Blaster relied on the fact that every copy of XP loads each of its components in the same location from computer to computer. Shuffling the deck with ASLR makes it much harder for the bad guys to write a worm that targets every copy of Vista.

9. Centralize events with Event Viewer. XP's event logs are useful for keeping track of your computers, but every computer maintains its own logs. Managing dozens of desktops means either wearing out a lot of shoe leather or buying a third-party event-log aggregator tool. Vista's Event Viewer, in contrast, lets you centralize any of a group of systems' events to a single system.

10. And lots more! Resize existing disk partitions with Vista's Disk Manager. Put eight gigs of RAM on your system and see—and use!—all of it. Easily tell Vista to send you an email message if a particular event occurs. Eliminate LAN Manager hashes, that persistent 1980s security hole, once and for all. Take advantage of ReadyDrive and Intel Turbo Memory for a system that comes out of hibernation in just 12 seconds. Give Vista a close look, and you'll find lots of things to like!

InstantDoc ID 99986



Mark Minasi
(www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex). He writes and speaks around the world about Windows networking.

10 Reasons *Not* to Deploy Windows Vista

With these irritating problems, why would any company make the switch?

by Alan Sugano

With a weak economy, businesses need to do more with less. When it comes time to consider upgrading a Windows XP environment to Windows Vista, many companies are choosing not to. Ultimately, upgrading has to make business sense, and many companies find the cost to upgrade outweighs any benefits they receive. Here are my top 10 reasons why companies are staying away from Vista.

1. Vista requires new hardware or significant hardware upgrades. To get acceptable performance on Vista, you're probably looking at significant hardware upgrades, if not a new computer. In my work environment, we've found the minimum requirement for a Vista desktop is 2GB of memory, a dual-core processor, 80GB hard disk drive, and a video card with at least 256MB of VRAM. For most users, these specs mean getting a new computer because upgrading an existing system isn't cost effective.

2. The additional cost of additional upgrades. There's a good chance you'll have to upgrade your applications as well. Unless you're running the latest version of your application, you'll probably need to upgrade—or at the very least install a patch—for Vista compatibility. Application upgrades could cost thousands of dollars per desktop, depending on the number and type of applications your company's running. Make sure you check for compatibility and upgrade problems before committing to upgrading your entire company.

3. Compatibility problems with applications. Even with the latest updates, you might still encounter compatibility problems with some applications. You might even be forced to change applications if the vendor doesn't plan to support Vista. VPN clients, accounting applications, faxing applications, and some graphics programs have caused problems in my environment.

4. Training costs. With the upgrade from Windows 2000 to XP, users could pretty much figure things out on their own. With Vista, you might not be so lucky. Many programs and utilities have been moved in Vista, and your users might have a difficult time locating them. When I first started using Vista, I wanted to view my installed applications. I launched Control Panel and looked for Add/Remove Programs, but it wasn't there. I eventually found the applet—renamed Programs and Features—but the search added to the frustration of getting up to speed with Vista.

5. Vista requires significant tweaks. Changes to User Account Control (UAC), local user rights, and application settings might be necessary to get your company's applications to run on a Vista computer. Most of these settings can be controlled with Group Policy; however, finding which settings to change can be the real headache.

6. Boot times and the patch installation process. This is one of my pet peeves: Even with a fast computer, Vista is slow booting up. Vista SP1 has helped somewhat, but when I'm waiting for Vista to boot, all I can think about is how fast my machine would be if it were running XP. During some patch installations, Vista installs the patch, reboots, runs another process to complete the patch installation, then reboots again before you can use your computer. I always seem to get hit with the double-boot patch installation at the beginning of meetings, so everyone has to wait while my machine completes the patch process before I can show my PowerPoint presentation.

7. Laptop performance problems. Properly configured, the current generation of desktop computers generally has acceptable performance running Vista. However, if you have a laptop—especially a subnotebook—you could encounter performance problems. You might need to disable some of the features on Vista, such as Aero, to obtain acceptable performance.

8. Windows XP works well. XP is stable, and it's more compatible with existing applications than Vista. Vista is arguably more secure, but some of the security features, such as UAC, can be so irritating that companies end up disabling them. XP isn't perfect, but it still works acceptably for most users, so many companies are hesitant to purchase an upgrade.

9. Limited payoff in productivity. Most people don't mind going through a learning curve if there's a significant payoff. Vista has some nice features; however, in my organization, we haven't experienced a big productivity payoff after getting up to speed with it. In contrast, there's a significant learning curve with Microsoft Office 2007 because of the changes to the UI. But after getting up to speed with Office 2007, I can honestly say that I create documents faster and more easily than before. I haven't experienced any similar benefit with Vista. At the end of the day, upgrading has to make business sense.

10. Windows 7 isn't far away! In my opinion, Microsoft realized it missed the mark with Vista and is now scrambling to get the next release of Windows out. I think many companies are waiting to see the new features in Windows 7, currently scheduled to release in 2010, and might just skip Vista altogether. Vista is looking more and more to me like Windows Me all over again.

InstantDoc ID 99988



Alan Sugano
(asugano@adscon.com) is the president of ADS Consulting Group, which specializes in networking, custom programming, Microsoft .NET web development, and SQL Server development. He's the author of *The Real-World Network Troubleshooting Manual* (Charles River Media).

Does Anonymous Web Surfing Leave You in the Dark?



iPrism Web Filter Stops Anonymizers Cold

SC MAGAZINE ★★★★★ 2008

Anonymizers are emerging as the perfect way for people to avoid Web filters. They are also the perfect portal for dangerous malware, spyware, viruses and other Web-based threats to attack your networks. iPrism Web Filter sheds light on anonymous surfing with the ultimate in anonymizer threat protection:

- Real-time anonymizer updates
- Deep Packet Inspection
- Blocks SSL Spoofing
- Dynamic proxy detection
- Active Domain IP Address Mapping



iPrism h-Series Web Filter

STBERNARD

Sign Up For a Live Demo and Get a Cool T-Shirt

Visit www.stbernard.com/Anonymizer or Call 800-782-3762

Controlling Your Code's Flow with PowerShell's Conditional Statements

by Robert Sheldon



Windows PowerShell provides several ways to control the flow of code, including the *if*, *for*, and *while* statements. You can use these three statements to define conditions and the actions to occur when those conditions are met. You can even specify the actions to occur when a condition isn't met. Let's look at the various components that make up the *if*, *for*, and *while* statements and how to use each type of statement for tasks such as retrieving a list of text files in a folder and retrieving a list of processes and the number of handles they're using.

Lesson 2 in the PowerShell 201 series explores how to use the *if*, *for*, and *while* statements

The *if* Statement

An *if* statement contains a conditional code block, which is enclosed in parentheses, and a script block, which is enclosed in braces. The conditional code block specifies a condition, whereas the script block specifies one or more actions. When the condition is met—that is, when the conditional code block evaluates to true—PowerShell runs the script block. When the conditional code block evaluates to false, PowerShell skips the script block.

For example, the following code initializes the $files variable, then defines a basic *if* statement:

```
$files = dir c:\archivedfiles\*.txt
if ($files -ne $null)
{
  "There are files in this folder."
  write-host
}
```

The first line assigns a collection of text files to $files. The *if* statement uses the $files variable in its conditional code block ($files -ne $null) to specify that the variable must not be null. In other words, the variable must contain text files. When there are text files, the conditional code block evaluates to true and the script block runs and displays the message *There are files in this folder.* When the conditional code block evaluates to false, the *if* statement ends. As a result, no message is displayed when the folder doesn't contain text files.

At times, you might want to take a specific action when a conditional code block evaluates to false. You can do so by adding an *else* clause. This clause begins with the keyword *else*, followed by its own script block. The *else* script block runs when none of the *if* statement's conditional code blocks evaluate to true. Take, for example, the following *if* statement:

```
$files = dir c:\archivedfiles\*.doc
if ($files -ne $null)
{
  "There are Word " +
  "files in this folder."
  write-host
}
else
{
  "No Word files in this folder."
  write-host
}
```

When the conditional code block ($files -ne $null) evaluates to false, the else script block runs and displays the message *No Word files in this folder.*

In this example, the *if* statement takes into account two scenarios: the folder contains Microsoft Word files or doesn't contain them. However, there might be times when you want the statement to handle more than two scenarios. In these situations, you can add a few *elseif* clauses. (If you need to use many *elseif* clauses, you should consider using a *switch* statement, which I'll discuss in the next lesson.) For each *elseif* clause, you define a conditional code block and a script block. When the conditional code block evaluates to true, the script block runs.

For example, the code in Listing 1 uses *elseif* clauses to determine how many files are in a folder. In this code, one *if* statement is embedded in another *if* statement. The code begins by assigning a collection of text files to $files. The outer *if* statement then checks to see whether $files is null. I perform this check rather than using the Count property to determine the number of files because I had to provide for the possibility that there might be only one file in the folder. The Count property is available only when there's two or more files in a folder. When there's more than one file, PowerShell treats $files as an array, which supports the Count property. When there's only one file, Power Shell treats $files as a scalar (i.e., single) value, which means the Count property isn't available.

When the outer *if* statement finds that $files is null, the else clause in callout B runs. This clause's script block displays the message *No files in folder.* When $files isn't null, the inner *if* statement in callout A runs. The inner *if* statement's conditional code block defines three conditions: an *if* condition and two *elseif* conditions.

Listing 1: An *if* Statement That Contains *elseif* Clauses

```
$files = dir c:\archivedfiles\*.txt
if ($files -ne $null)
(A){
  if ($files.count -gt 10)
  {
    "More than 10 files in folder."
    write-host
  }
  elseif ($files.count -gt 7 -and
    $files.count -le 10)
  {
    "8-10 files in folder."
    write-host
  }
  elseif ($files.count -gt 4 -and
    $files.count -le 7)
  {
    "5-7 files in folder."
    write-host
  }
  else
  {
    "Fewer than 5 files in folder."
    write-host
  }
}
(B)else
{
  "No files in folder."
  write-host
}
```

Learning Path

***WINDOWS IT PRO* RESOURCES**

To read the previous lesson in the PowerShell 201 series, go to

"Iterating Through Collections with PowerShell's foreach Loops," InstantDoc ID 99873

Listing 2: An *if* Statement That Contains an Embedded *foreach* Statement

```
$files = dir c:\archivedfiles\*.txt
if ($files -ne $null)
{
  write-host
  foreach ($file in $files)
  {
    "The $file file is " +
      $file.length + " bytes."
  }
  write-host
}
else
{
  "No files in this folder."
  write-host
}
```

The *if* condition ($files.count -gt 10) specifies that the number of text files must be greater than 10. When this conditional code block evaluates to true, the script block displays the message *More than 10 files in folder.*

The first *elseif* condition ($files.count -gt 7 -and $files.count -le 10) specifies that the number of text files must be greater than 7 but less than or equal to 10. When this

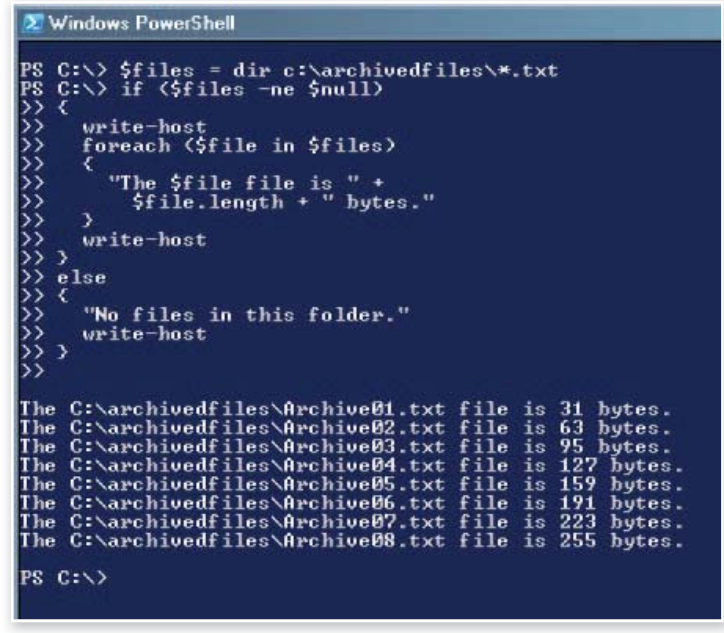


Figure 1: Sample results from embedding a *foreach* statement in an *if* statement


ECONOMY
MEETS
ECOLOGY.
With energy consumption expected to double in five years, how do you build and manage your IT to reduce costs? Greener software: a complete range of energy-efficient software to optimize your infrastructure, boost business process efficiency and implement truly responsible collaboration. A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
Get our green strategy whitepaper at ibm.com/green/software
IBM
IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml. © 2008 IBM Corporation. All rights reserved.

conditional code block evaluates to true, the script block displays the message *8-10 files in folder.*

The second *elseif* condition ($files.count -gt 4 -and $files.count -le 7) specifies that the number of text files must be greater than 4 but less than or equal to 7. When that conditional code block evaluates to true, the script block displays the message *5-7 files in folder.*

If none of the three conditional code blocks evaluate to true, the *else* clause's script block runs. It displays the message *Fewer than 5 files in folder.*

As Listing 1, page 42, demonstrates, you can embed *if* statements in the script block of another *if* statement, but you aren't limited to embedding only these types of statements. You can, for example, embed a *foreach* statement in an *if* statement's script block, as shown in Listing 2, page 42. The *foreach* statement runs only when the *if* statement's conditional code block evaluates to true. In other words, when the folder contains text files, the *foreach* statement will loop through those text files. Each time a loop runs, *foreach* returns the text file's size, as Figure 1, page 42, shows.

The *for* Statement

In Lesson 1, I showed you how to implement *foreach* loops to iterate through a collection. You can also use *for* statements to loop through collections. A *for* statement implements a counting loop that iterates through a collection as long as the condition is true. Like *if* statements, *for* statements include a conditional code block and a script block. However, the *for* statement's conditional code block is more complex.

Let's take a look at a simple example. The following *for* statement displays the values assigned to the $a variable:

```
for ($a = 1; $a -le 5; $a++) {$a}
```

The statement begins with the keyword *for*, followed by the conditional code block ($a = 1; $a -le 5; $a++). The *for* statement's conditional code block is made up of three parts, which are separated by semicolons. The first part ($a = 1) initializes the $a variable with the value 1. The $a variable provides a base value, or starting value, for the other code block elements.

The second part ($a -le 5) is the condition itself. In this case, the value in $a must be less than 5 to evaluate to true. The third part ($a++) increments $a by 1 at the end of each loop. As a result, the statement will continue to step through the collection as long as the value in $a is less than or equal to 5. When $a equals 6, the *for* statement ends. Figure 2 shows sample output from this statement.

In some cases, you won't know the number of elements in a collection. The code in Listing 3 demonstrates how you can use a *for* statement to iterate through such collections. This code begins by storing a collection of text files in the $files variable. The *if* statement uses the $files variable and its Count property ($files.count) to check the file count. As I mentioned previously, if there's only one file in the collection, PowerShell returns an object (i.e., a System.IO.FileSystemInfo object) that has a scalar value. If there are no files, PowerShell doesn't return an object. In either case, the Count property doesn't exist. As a result, you receive a null value if you try to call the Count property, which is why you can use it as a condition in the *if* statement.

When $files.count returns a null value, the *elseif* clause in callout B checks for the condition of there being only one file. If this condition isn't met, there are no files and the *else* clause in callout C runs.

When $files.count doesn't return a null value (i.e., PowerShell returns a System.Array object so the Count property exists), the code in callout A runs because there are at least two files. In callout A, the embedded *for* statement's conditional code block uses the Count property to determine the exact number of files (i.e., elements) in the collection. As long as $i is less than the number of elements, the condition evaluates to true.

Note that I initialize $i to 0. I use 0 because collections (such as $files) use base 0 indexing. In the script block, I use $i to specify which element to retrieve from the collection. For instance, during the first loop, $i is set to 0. This means that $files[$i] is the same as $files[0]. On the second loop, $i equals 1, so the value becomes $files[1], and so on. Figure 3 shows sample results from the code in Listing 3.

One other item worth pointing out is that you can declare and initialize the base variable before the *for* statement.

Listing 3: A *for* Statement

```
$files = dir c:\archivedfiles\*.txt
if ($files.count -ne $null)
A{
  for ($i = 0; $i -lt $files.count;
    $i++)
  {
    $files[$i].name + " = " +
      $files[$i].length + " bytes"
  }
  write-host
}
Belseif ($files -ne $null `
    -and $files.count -eq $null)
{
  $files.name + " = " +
    $files.length + " bytes"
  write-host
}
Celse
{
  "No text files in this folder."
  write-host
}
```

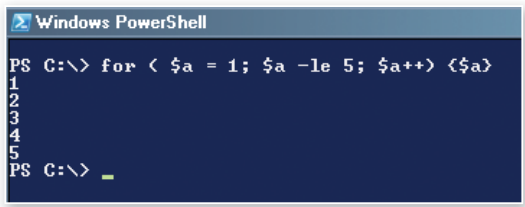


Figure 2: Sample results from using a *for* statement to loop through a collection

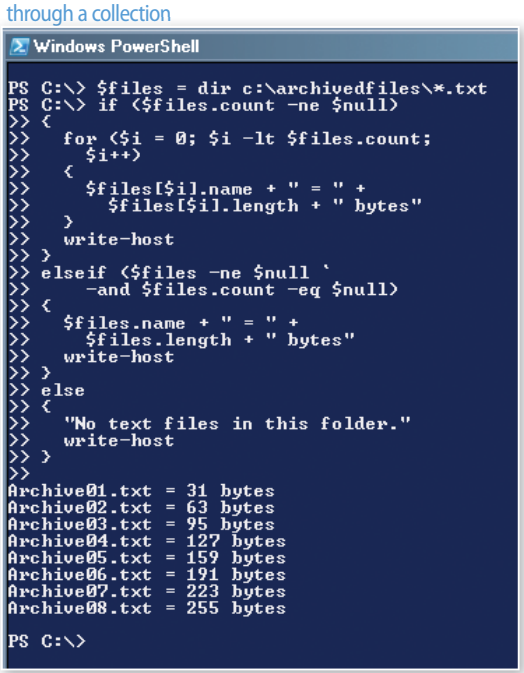


Figure 3: Retrieving a list of text files and their sizes



IBM, the IBM logo, ibm.com and Smart SOA are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml. Other company, product and service names may be trademarks or service marks of others. © 2008 IBM Corporation. All rights reserved.

For example, in Listing 4, the $i variable is declared and initialized in the line highlighted by callout A. As you can see, the code is easier to read with this setup.

The *while* Statement

Like the *for* statement, the *while* statement is a type of loop that iterates through a collection. The *while* statement, which consists of a conditional code block and a script block, continues as long as the conditional code block evaluates to true. The following code provides a simple example of how this works:

```
$count = 0
while ($count -lt 5)
{
  $count++
  "The count is
  $count."
}
```

The first line of code initializes the $count variable to 0. This variable is used as a base or starting value for the looping. The conditional code block ($count -lt 5) specifies that $count must be less than 5.

Listing 4: Code That Declares and Initializes $i Before the *for* Statement

```
$files = dir c:\archivedfiles\*.txt
$i = 0                                    (A)
if ($files.count -ne $null)
{
  for ($i; $i -lt $files.count;
    $i++)
  {
    $files[$i].name + " = " +
      $files[$i].length + " bytes"
  }
  write-host
}
elseif ($files -ne $null `
    -and $files.count -eq $null)
{
  $files.name + " = " +
    $files.length + " bytes"
  write-host
}
else
{
  "No text files in this folder."
  write-host
}
```



Figure 4: Retrieving a list of processes and the number of handles used

When the conditional code block evaluates to true, the script block runs. The first statement in the script block increments $count by 1. The second statement outputs a string that displays the running value in $count, as shown in the results:

```
The count is 1.
The count is 2.
The count is 3.
The count is 4.
The count is 5.
```

Note that when $count is 4 in the conditional code block, the script block increments $count by 1 and displays a value of 5 in the output. It's not until the next time through the loop that the conditional code block evaluates to false, ending the *while* loop.

Sometimes you might not know the number of elements in a collection that's being iterated through with a *while* loop. In this situation, you can use the Count property to retrieve that value:

```
$proc = Get-Process
$count = 0
while ($count -lt
$proc.count)
{
  "The " +
    $proc[$count].name +
    " process uses " +
    $proc[$count].handles +
    " handles."
  $count ++
}
```

This code first assigns the results of the Get-Process cmdlet to the $proc variable. This cmdlet returns a list of processes running on the local system. The conditional code block in the *while* loop specifies that the value in $count must be less than the total number of processes ($proc.count). Figure 4 shows sample results from running this code. As you can see, you can use the $proc variable to retrieve not only the number of processes but also each process's name and number of handles.

Moving Forward

In this lesson, you learned about the *if*, *for*, and *while* statements. These statements, along with the *foreach* statement and ForEach-Object cmdlet discussed in Lesson 1, provide a wide range of tools for implementing flow-control statements. You should try out all these statements and try to combine them in different ways, such as adding *if* statements to *foreach* statements. The more comfortable you become with using these statements, the better you'll understand them and be able to implement them in your code.

InstantDoc ID 100141



Robert Sheldon
(contact@rhsheldon.com) is a technical consultant and author of material about Windows, relational database management systems, and business intelligence design and implementation. His latest book is *Beginning MySQL* (Wiley). Find out more at www.rhsheldon.com.



IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml. © 2008 IBM Corporation. All rights reserved.

Virtualization
Cloud Computing

Share Excel Spreadsheets on the Web

eXpresso has released **eXpresso**, a solution that lets users upload .xls spreadsheets to a secure server so that users can form communities to work on the spreadsheets interactively. eXpresso offers version tracking, email alerts when a spreadsheet is accessed or edited by a community member, and IM between community members. eXpresso is compatible with Office 2007/2003/XP/2000 but supports only the .xls format (i.e., Excel 97–2003 workbooks). The product comes in two versions: eXpresso, which is free, and eXpresso Pro, which is $15 per month or $79 per year (group discounts are available) and is available as a 30-day free trial. For more information, contact eXpresso at 650-320-1730 or visit www.expressocorp.com.

EventTracker 6.2 Secures USB Data

Prism Microsystems announced an update to its **EventTracker** log- and change-management application. EventTracker 6.2 monitors USB device insertion and removal and tracks all data that's modified, copied to, or deleted from such devices. When EventTracker detects unauthorized use of USB devices, it can disable the device and alert admins. EventTracker can help you track an internal data breach to a specific user, system, or time; can launch remedial action locally on a Windows workstation or server in response to an event, and has support for Windows Server 2008. To learn more, call 410-953-6776 or visit www.prismmicrosys.com.

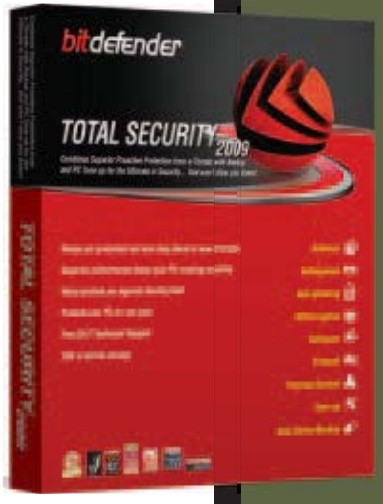
iStor Ships Virtual Storage Manager

Virtual storage vendor iStor Networks announced that it has released **integraSuite/MC Management Center**, an application that lets administrators manage their iStor storage products from a single console. The application eliminates the need for RAID group and LUN configurations to be managed individually and presents available storage as a generic pool that can be divided up into custom volumes. "The integraSuite Management Center was developed using extensive user feedback, with the goal of minimizing the time users spend allocating and managing their storage while increasing their storage efficiency," said Robert Friend, director of product marketing for iStor Networks. "iStor's unique virtualized storage functionality further enhances the customer experience with usability features not available with traditional architectures." For more information about iStor, go to www.istor.com.

Security

Prevent an Array of Internet Threats

Security solutions provider BitDefender recently launched **Bit Defender Total Security 2009.** This software protects against viruses, spyware, hackers, spam, and other e-threats without slowing performance. Rather than relying on virus signatures, the product uses heuristics to identify and block new and zero-day threats. In addition, BitDefender Total Security 2009 lets you back up data online, provides a laptop mode to extend battery life, offers IM encryption, and enables secure local storage. For more information, contact BitDefender at 954-776-6262 or visit www.bitdefender.com.



InstantDoc ID 100139



Jeff James | jjames@windowsitpro.com
Editor's Note: Send new product announcements to products@windowsitpro.com.

PRODUCT SPOTLIGHT

Citrix Unveils XenApp 5

Citrix Systems has released **XenApp 5**, the latest version of its application virtualization product. Previously known as Citrix Presentation Server, XenApp 5 is the latest upgrade to the Citrix Delivery Center product family, which includes XenDesktop, XenServer, and XenApp. XenApp 5 supports Windows Server 2003 and



provides easy migration to Windows Server 2008. (XenApp 4.5 and earlier versions of XenApp are not compatible with Server 2008.)

According to Bill Hartwick, senior director of product marketing for Citrix's application virtualization group, XenApp 5 features improved performance monitoring, a streamlined interface, and faster application start-up times than XenApp 4.5. A preferential load-balancing feature allows administrators to have fine-grained control over application workload prioritization, which improves overall performance and responsiveness. For more information on XenApp, call 954-267-3000 or visit www.citrix.com/xenapp.


GIANT LEAPS.
SMALL
FOOTPRINTS.
With the world's data growing dramatically, IBM storage virtualization solutions can help you gain control in a responsible, energy-efficient way. The IBM System Storage™ SAN Volume Controller can reduce storage growth by up to 20% and boost utilization by as much as 30%. And combined with IBM tape solutions, some companies have reduced their TCO by as much as 50%[1]. A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
Get our storage virtualization whitepaper at ibm.com/green/info
IBM
[1]TCO estimates based on IBM internal study. IBM, the IBM logo, ibm.com and System Storage are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.
© 2008 IBM Corporation. All rights reserved.

Another Day, Another Crisis?

The Common Denominator in Performance Nightmares

Just Another Day at the Office

You've probably had it happen, and there's nothing quite like it. First thing Monday morning, a "MUST be handled before noon!" list of emergencies hits you in the face:

- The sales manager is squawking because the CRM database is slow
- Accounting is nagging because email is slow
- The NAS server is averaging unacceptably high counts of queued disk I/Os
- You're getting constant poor performance alerts from the SAN
- Backups have not been completing during the backup window



These nagging, ulcer-creating problems are also the subject of several emails from the CFO because, on top of being bad for company production, in this time of economic uncertainty they're also bad for business. Work is being slowed down and the company is losing money.

The Culprit

The common hardware denominator to all these crises is the hard drive—the slowest link in a computer system. If the data on a hard drive is fragmented, that already dragging weakest link becomes agonizingly slower.

With frenetic requirements for continuous data access, enormous files and huge disk capacities, fragmentation is worse than ever; files in hundreds or even thousands of fragments aren't at all uncommon. Brett Taylor, of Van Wert Medical Services, discovered just how bad it can get. "Our electronic medical records server is a Microsoft® SQL Server® and one day it came to a halt," he says. "I did everything: ran spyware software, deleted numerous temp files, ran Windows® update, etc. but nothing would allow the server to run. It turned out that the hard drive was horribly fragmented."

Craig Merchant of Pace Engineering, San Francisco, discovered very similar problems. "I get a huge amount of fragmentation when I run multiple virtual machines on my system using VMware®," he reports. "I've had as much as 20% fragmentation that the Windows defrag utility couldn't get rid of. In my experience, virtual machines fragment their disks as much as real machines. But Windows systems running VMware tend to have extreme fragmentation problems, particularly when running multiple VM's."

Making Mondays Go Away

Making the right defragmentation technology choice in today's frantic fragmentation environment is vital. Scheduled defragmentation has become a problem due to the IT hours required to schedule defragmentation and the downtime required for the defragmenter to run. But worst of all, scheduled defragmentation is no longer fully addressing fragmentation.

The only solution that stands up to today's escalating fragmentation is Diskeeper®. Diskeeper's proprietary InvisiTasking® technology makes for completely automatic, invisible defragmentation. Because it utilizes otherwise idle resources, it requires absolutely no scheduling, freeing up IT time for more important tasks. There is never a negative performance hit during defragmentation, and system performance and reliability are consistently maximized.

Reliability and Performance Issues Become Nonexistent

Mike Driest, Network/Systems Administrator for Industrial Control Repair in Warren, Michigan, has found Diskeeper to be the only solution. "Automatic disk defragmentation for a server is like oil for the engine in your car," he says. "One of the most useful features about Diskeeper, when using it on our 20+ servers, is the automatic defragmenting with InvisiTasking. Diskeeper helps all of our servers (Domain Controllers, File, Exchange, SQL, Web, etc.) perform at their very best. Reliability and performance issues relating to a lack of defragmentation do not exist in our environment."

Diskeeper has proven the solution for Andrew Wise, Senior Network Engineer at Datacore Marketing in Westwood, Kansas as well. "We run Diskeeper primarily on our SQL database servers with Fibre Channel SAN connectivity," he says. "It keeps the database and log files defragmented at the OS level to reduce the I/O on our SAN. After installing Diskeeper and doing a full defrag, we noticed around 10–15% reduction in the amount of I/O generated and in the amount of time it took for the SAN to service each request. We are a Microsoft SQL Server database shop and we process terabytes of SQL data on a daily basis, so any reduction in the amount of time it takes to do that processing saves us money."

Diskeeper with InvisiTasking makes for smooth, calm Monday mornings for these and thousands of other enterprises the world over. Take advantage of our special offer and find out, free of charge, what it can do for you.

SPECIAL OFFER:

Discover how vital Diskeeper with InvisiTasking is to you.

Get your FREE fully operational trial version for 45 days now! (Extended from 30 days)

Download at:

www.diskeeper.com/tryitfree

Volume licensing and Government/Education discounts are available by calling 800-829-6468, extension 4149.

with InvisiTasking®
Diskeeper® 2008
Maximizing Performance and Reliability—*Automatically*™

Diskeeper corporation

© 2008 Diskeeper Corporation. All Rights Reserved. Diskeeper, InvisiTasking, Maximizing Performance and Reliability—Automatically, and the Diskeeper Corporation logo are either registered trademarks or trademarks owned by Diskeeper Corporation in the United States and/or other countries. All other trademarks and brand names are the property of the respective owners. Diskeeper Corporation • 7590 N. Glenoaks Blvd. Burbank, CA 91504 • 800-829-6468 • **www.diskeeper.com**

James

"In a small company, Exchange can be the equivalent of building a Patriot missile battery to kill a few fruit flies."



Who Says You Need Microsoft Exchange Server?

For SMBs, low-cost Exchange alternatives offer less costly (and less complex) messaging solutions

Along with Microsoft Office, Microsoft SharePoint Server, and Microsoft SQL Server 2008, Microsoft Exchange Server is clearly one of the most successful Microsoft product families in recent memory. The Redmond juggernaut has swatted aside its competitors in the enterprise messaging market, effectively planting a Microsoft flag on a smoldering pile of cracked Lotus Domino and Novell GroupWise installation CDs. According to Mark Levitt, VP of collaboration and enterprise 2.0 strategies at market research firm IDC, Microsoft Exchange/Outlook grabbed 52 percent of the worldwide integrated collaborative environment license and maintenance revenue in 2007. The next biggest player was IBM Lotus Domino/Notes with a 38 percent share. Exchange is on a roll, and big enterprises seem keen to jump aboard.

But it's also true that Exchange has evolved into a complicated product that can be overkill for many small businesses. It's no secret that Microsoft frequently looks to its largest customers in the Fortune 1000 for the lion's share of input on new product releases—a product-development methodology that has made Exchange a powerful resource in companies that have more than 500 employees but an arguably extravagant investment (in time and resources) for smaller businesses. In a small company, Exchange can be the equivalent of building a Patriot missile battery to kill a few fruit flies. Microsoft is coming under increasing pressure on the low end of the market from web-based email and groupware alternatives (e.g., Gmail, GMX, Yahoo! mail) and has sought to fight back with low-cost hosted Exchange services of its own. Microsoft also offers Small Business Server (SBS) and Essential Business Server (EBS), small business products that bundle Exchange with other Microsoft business applications.

But what if you're an IT pro who doesn't need or want Exchange, and you don't want to put your communications infrastructure on someone else's mail server? A number of options are available, including PostPath Server and Kerio Mail Sever (KMS). Cisco recently announced that it would acquire PostPath, a Boston-based developer that makes the eponymous PostPath Server, a Linux-based, drop-in Exchange replacement. The move gives Cisco a viable competitor to Exchange in the enterprise but also helps Cisco bolster its cloud computing–based Software as a Service (SaaS) strategy.

"[Cisco knows] that bold steps are needed to shake the lock-in that Microsoft, IBM, and other email vendors have on enterprises," said Levitt. "Cisco is leading with the innovation that is possible with SaaS and the broader, higher-scale cloud-computing model, for which a comprehensive strategy is currently being formulated at Cisco to enable it to become a broad business and IT solutions provider in the cloud."

Did You Know?

IT market research firm Gartner, Inc. estimates that Microsoft Exchange will have a 70 percent market share in the enterprise email and collaboration segment by 2010.

An attractive Exchange alternative for smaller businesses is KMS, a product positioned at the lower end of the messaging market. "Some installations [of KMS] are as small as five users," said Dusan Vitek, vice president of worldwide marketing for Kerio. "Many of our customers believe that email is too critical to be outsourced … and that the inability to access email when not connected to the Internet is a big negative for them." Vitek mentioned that most of Kerio's customers fall into the 10-500 seat range. According to Vitek, switching to KMS also can save IT professionals money over a comparable Exchange installation: Kerio's 50-user minimum licensing cost is only $1,299, whereas a comparable Exchange 2007 installation weighs in at $5,418.

KMS runs on Windows Vista/2003/XP/2000, Red Hat Linux, Fedora, SUSE, and Mac OS X. It also works with Outlook (via an Outlook Connector) and supports mobile devices such as Windows Mobile smart phones, Research in Motion (RIM) BlackBerry devices, and Apple iPhones. An Exchange-to-KMS migration tool is also available.

Akis Fotakelis, a systems administrator and *Windows IT Pro* contributor, has used KMS and praised its low cost, ease of use, and ability to integrate with Active Directory (AD). Fotakelis said that KMS was also considerably less expensive than other SMB email solutions he considered—a point that was a big factor in his purchase decision. "The price was a real bargain," Fotakelis said. "Not only could I install it on a workstation, saving the license for a Windows server, but I saved money from buying separate programs for antispam, antivirus, backup, archiving, monitoring, and mailing-list management."

InstantDoc ID 100311

JEFF JAMES (jjames@windowsitpro.com) is senior editor, products, for *Windows IT Pro* and *SQL Server Magazine*. He specializes in virtualization and terminal services and has over 15 years of experience as a writer and digital-content producer.

Introducing an integrated approach to complete SharePoint protection and management

DocAve™ Software for SharePoint

Changing the way Administrators manage SharePoint



FREE 30 DAY TRIAL
Download at
www.avepoint.com

SharePoint management made simple.

Now you can control and manage the back-end of all your SharePoint environments from one place. DocAve is the only truly integrated, easy-to-use software that offers a complete set of SharePoint backup, recovery, and administration tools. One solution, with many mix-and-match functions, now gives you power like never before.

Complete SharePoint protection.

With item-level backup and full-fidelity restore, DocAve allows for fast recovery of business critical documents and content. Complete SharePoint platform backup allows for quick and painless recovery of the entire system during a disaster. With DocAve, you'll have complete confidence in your SharePoint environment.

AvePoint

Call 1-800-661-6588 or visit www.AvePoint.com for more information or to download a free trial.

© AvePoint, Inc. All rights reserved. DocAve, AvePoint, and the AvePoint logo are trademarks of AvePoint, Inc. All other names mentioned are property of their respective owners.

SharePoint Backup Tools

Different solutions, unique benefits

by Curt Spanburgh

A friend of mine had a tree he wanted to prune. The task seemed straightforward, and he thought he had the right tools, but the tree had other ideas. A branch broke and hit my friend on the back of the head. My friend managed to call the ambulance before he passed out. This story just goes to show that there are some things you need help with—for example, recovering data on Microsoft Office SharePoint Server 2007 (MOSS 2007). As a SharePoint consultant, I commonly receive calls from clients who tried to deploy MOSS 2007 and failed. SharePoint is outside the realm of common experience in most IT departments, so third-party tools are often necessary to help you handle the new technology and avoid getting hit on the head by something that you didn't realize could cause a problem.

Backing up MOSS 2007 correctly is one of those hazards. I evaluated four of the current MOSS 2007 backup offerings on the market. Let's get started with the findings.

Recovery Manager for SharePoint

Quest Software's Recovery Manager for SharePoint focuses on data recovery rather than backup. To back up your sites and databases, you need to use either the built-in tools available on the Operations page of your SharePoint Central Administration page or the Stsadm command-line tool. Thus, using Recovery Manager requires knowledge of the built-in SharePoint backup tools. In fact, all the tools I evaluated require good knowledge of SharePoint and Microsoft SQL Server.

Recovery Manager runs as a component of Quest's Site Administrator for SharePoint, which is included in Recovery Manager and will run a helpful diagnostic of your environment as part of the installation process prior to deployment. The diagnostic will state what prerequisites are needed for a successful installation. Depending on the configuration of your SharePoint farm, there could be Active Directory (AD) and SQL Server security requirements that need to be satisfied. The installation wizard will help you take the necessary steps.

Once installed, Recovery Manager discovers the backups that you create on the SharePoint Central Administration page and analyzes them so they can be accessed for the restoration of objects. If a user accidentally deletes a file, Recovery Manager can find it in a previous backup and you can easily restore it via the Windows Server Backup-style UI shown in Figure 1.

Administrators sometimes discover that they installed SharePoint incorrectly, and the only fix is to reinstall it, even though they might already have moved thousands of files from the file server to SharePoint document libraries. One great Recovery Manager feature is its ability to retrieve files in the content databases and restore them

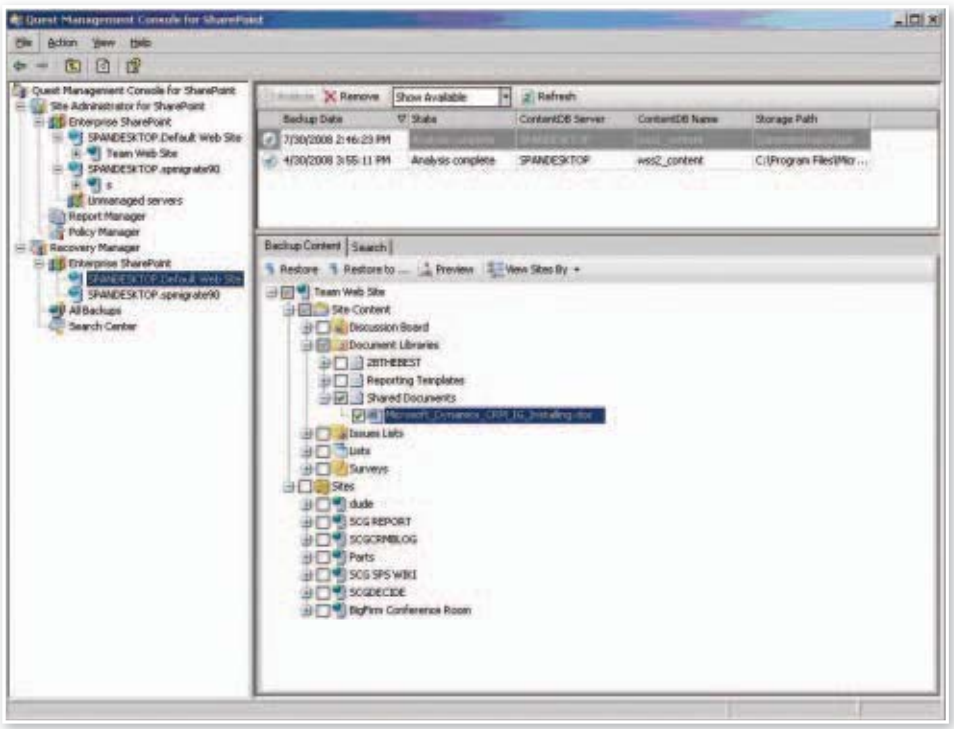


Figure 1: Recovery Manager's UI

to an NTFS folder, even if the SharePoint application server isn't working. This is a great get-out-of-jail-free card for seasoned as well as new SharePoint admins.

Recovery Manager for SharePoint

PROS: Allows granular recovery; can recover data from SharePoint databases; inexpensive; helpful installation process exposes problems before deployment; familiar interface

CONS: Requires a deeper-than-usual knowledge of SharePoint's administrative interface and command-prompt tools

RATING: ◆◆◆◆◇

PRICE: $49.95 per front-end server; request a quote at quest.com/products/request-a-quote-landing.aspx?requestdefid=14421

RECOMMENDATION: The uncomplicated interface and pared-down options make this a good, easy-to-use option for the junior administrator.

CONTACT: Quest Software • 949-754-8000 • www.quest.com/recovery-manager-for-sharepoint

DocAve 4.5

AvePoint's DocAve is much more than a SharePoint backup product, including as it does modules for administration, compliance, and migration, but I focus on its backup capabilities here. I tried to deploy DocAve without opening the over-300-page PDF, but I don't recommend it; several problems arose during installation that would trip up all but the most seasoned SharePoint admins. For example, I needed to create two SQL Server databases for the application to use, meaning that the installation account required SQL Server rights to create and access databases.

DocAve includes a complete backup and restore solution. DocAve is composed of three components: the server, the media server, and the client (i.e., the DocAve administration interface). All three components can be installed on the same server, but you wouldn't want to use DocAve for a single-server SharePoint deployment. This product is designed for extensive SharePoint deployments that use many scheduled backups that depend on demographic usage of site collections and individual sites and face the complexities that come with indexing large list and document libraries.

SQL DBAs are familiar with the concept of removing unwanted backups that waste disk space on NAS or SANs. In DocAve, this task is called *pruning*. DocAve schedules pruning with "pruning rules" that are much like a SQL Server maintenance plan.

Other features include the ability to back up load-balanced front end servers. You can perform live, incremental, and differential backups, as Figure 2 shows. A unique scheduling "ring" is prominent in the interface and allows quick access to backup schedules for multiple site collections. You can also encrypt and compress the backups using a configurable data security plan. Live job monitoring and email notification keep you informed of the state of your environment.

SharePoint's tools include some item-level backup ability, but DocAve goes further, letting you back up your SharePoint environment on every level, from the entire farm to a specific folder or list object. Restores can be as granular as an attachment, a document, or even a single version of a document—you can even restore an object's metadata.

The goal of DocAve is to do an entire backup of all the easy-to-miss parts of the SharePoint environment, including sites, web applications, content databases, index servers, and the all-important Microsoft IIS settings required to access the sites in the databases. DocAve also lets you perform backups according to the way users need the services, which helps reduce the load on the processors when people are working (e.g., you could exclude a site from the normal scheduled backup because you knew the COO has a meeting on that site this week).

There are several well-thought-out features under the Data Protection tab on the DocAve control panel, including an option to back up workflows, a schedule carousel for a 3D iPhone-like graphical view of scheduled backups for complex environments, and a pruning feature for setting backup intervals. With so many options available, some users might be overwhelmed. However, DocAve rewards the effort you put into learning its features in the form of methods to control backup times, storage media, and backup granularity. In short (and it's hard to be brief about this product), DocAve gives almost

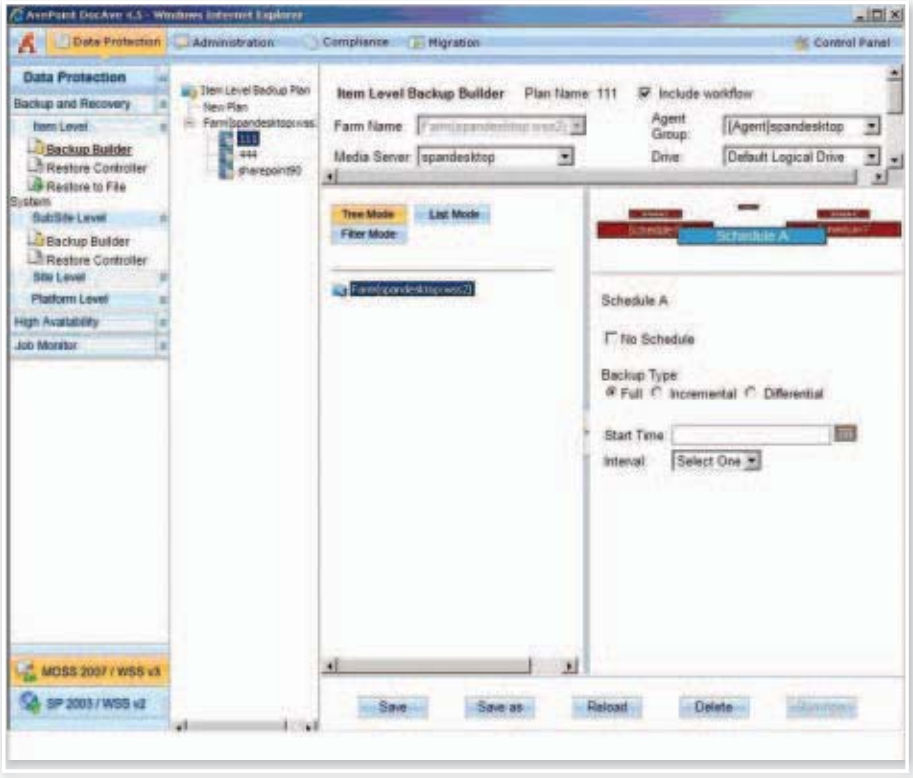


Figure 2. Selecting a backup type in DocAve

total backup control at all levels of the SharePoint farm. It's a good product for SharePoint admins who are thoroughly familiar with their farm and can adapt the tool to their infrastructure.

DocAve 4.5



PROS: The most complete package reviewed; has additional tools for site collection management

CONS: Difficult learning curve; giant user manual; expensive

RATING: ◆◆◆◆◆

PRICE: $2,995 per front-end server

RECOMMENDATION: If you have a large, complex, and busy SharePoint deployment, this is the package you want.

CONTACT: AvePoint • 800-661-6588 or 201-793-1111 • www.avepoint.com

Replicator for SharePoint Standard Edition

Syntergy Replicator for SharePoint addresses a part of the SharePoint world that the native product doesn't: replication of data to another SharePoint site and continuous synchronization of data between sites. If you have intercontinental offices or corporate partnerships that need to share their sites and document structures, Replicator fills that need. Often SharePoint administrators don't know how to bring together different sites, as in a corporate merger, without integrating the security of the companies. Replicator synchronizes library structures and version control across the enterprise, even if the collaboration is between different corporations with separate AD forests and the synchronization is bidirectional. For example, if a confidential document is checked out of a library in New York, a synchronized server in another company in London with a completely different AD domain will know about it in a very short time. If a site collection is lost in a corporate domain, the synchronized data acts like a hot spare of the lost libraries. You can even synchronize Web Parts in sites.

Replicator doesn't run as a separate application, but integrates into SharePoint's administration environment, as Figure 3 shows. Packet technology lets you control sessions over connections that might be interrupted, such as satellite links. For example, if a cruise ship were syncing its SharePoint server to a land-based server and the link went down, Replicator would hold the conversation until the link was reestablished. Likewise, you can publish documents to remote document libraries without worrying about failed or broken sessions. There's also a feature for scheduling replication and synchronization.

To reduce bandwidth usage, the Remote Differential Compression feature lets you transfer only blocks of data that have changed in the document being synchronized. As for document security, Replicator replicates user and group permissions along with permissions assigned to a SharePoint list and uses HTTP and HTTPS protocols to avoid infrastructure changes. Because all replication is event driven, crawlers aren't used and don't burden your front-end servers.

Replicator for SharePoint Standard Edition

PROS: Eliminates the need to upgrade marginal bandwidth for remote-site replication; offers a unique approach to disaster recovery by using replicates on other production servers as a recovery source; vendor works closely with customers to help with customization

CONS: Expensive; not a true backup and recovery solution

RATING: ◆◆◆◇◇

PRICE: $25,000 for the first two servers and $7,500 for each additional server

RECOMMENDATION: This product should be used in conjunction with one of the other products tested here for backup and recovery of granular data in your content databases. For the right scenario, it provides a layer of data integrity that's impossible with native tools alone.

CONTACT: Syntergy • 858-964-3243 • www.syntergy.com

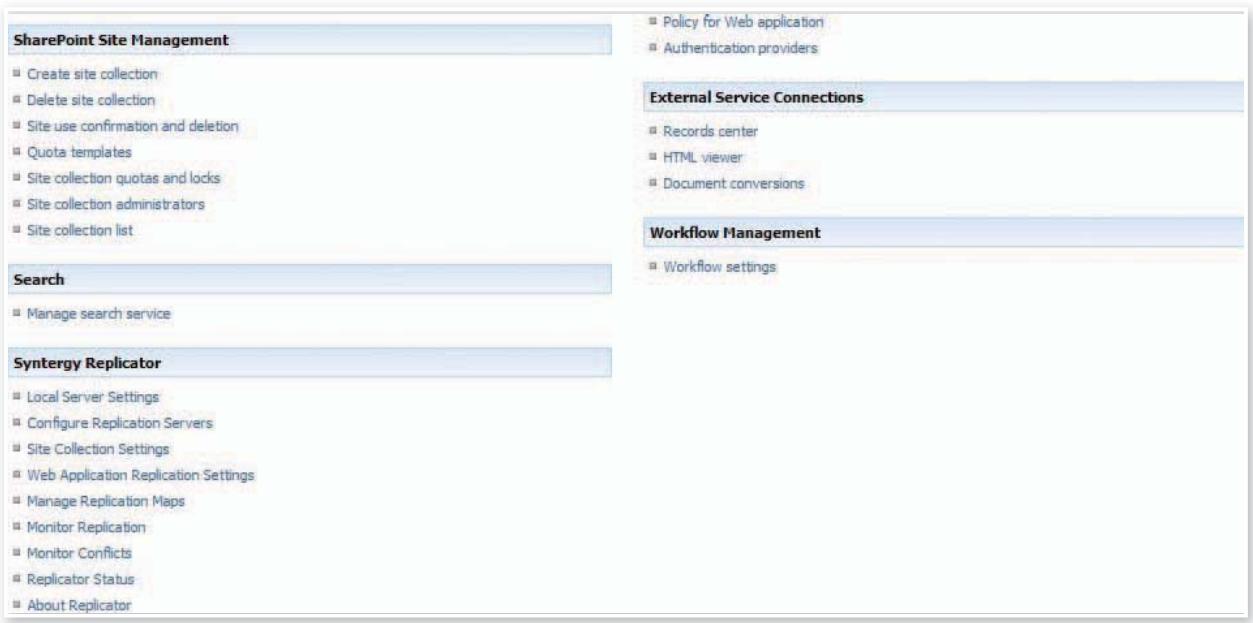


Figure 3. Replicator's SharePoint-integrated interface

SHAREPOINT BACKUP TOOLS

There seems to be no limit to the number of remote offices that Replicator can interactively replicate and synchronize. Even with bandwidth limitations, the product allows for a cohesive collaboration model—imagine the server room on a luxury cruise liner as a replication site connected to the home port. I couldn't test that scenario, of course, but it should get the attention of decision makers if their SharePoint deployment resembles this model.

Another possible way to use Replicator is to synchronize to a nonproduction SharePoint server that's used as a backup for a large development project that involves constantly changing functional specs, code updates, and business requirements. Syntergy provides a reduced price when Replicator is used in this way.

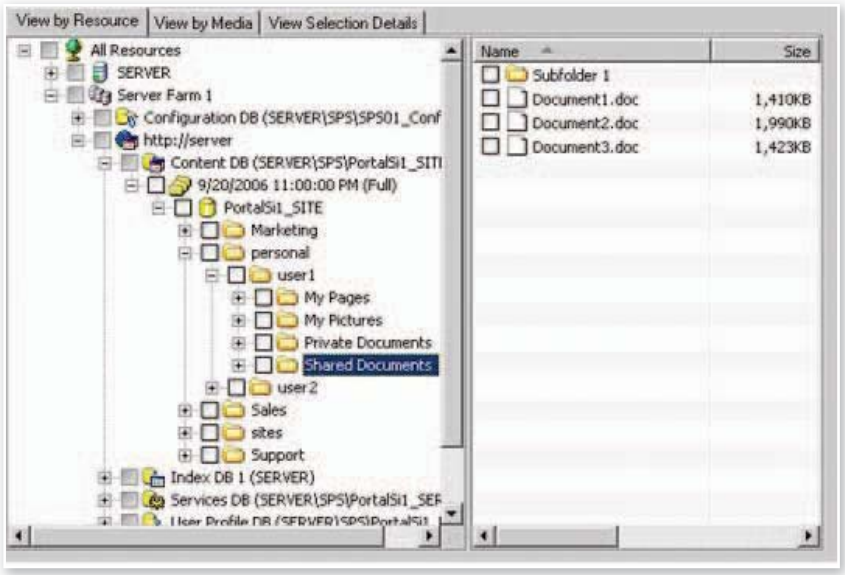


Figure 4. Backup Exec Agent for SharePoint's interface

Backup Exec Agent for Microsoft SharePoint

Many shops already have an enterprise backup system in place and prefer to extend that investment rather than deploy a separate product. Symantec's Backup Exec is almost ubiquitous as a backup solution in the enterprise, so it's a real boon to all those customers that Symantec has released an agent for SharePoint environments.

Backup Exec Agent for Microsoft SharePoint supports all versions since (and including) SharePoint 2001, making it a good choice for sites that haven't migrated because you can use the same backup agent after you upgrade your SharePoint farm. Backup Exec Agent for Microsoft SharePoint also is a good economic choice because it includes the backup agent for Microsoft SQL Server, which lets you back up the entire SharePoint farm first and perform the more granular restores later for those special circumstances when individual objects need to be retrieved.

The agent supports both 32-bit and 64-bit platforms and deployments ranging from small shops to server farms. The number of SharePoint backup agents will depend on the number of SharePoint front-end servers you deploy. You will need one agent per server, plus a Backup Exec Remote Agent, which allows normal backup of your operating system and the more conventional data that might be on your server.

The interface, shown in Figure 4, is familiar, which makes for an easy learning curve for already busy administrators. Like Recovery Manager for Sharepoint and DocAve, Symantec designed this agent to deal with the reality that restoration involves mostly individual items, concentrating on granular retrieval, including document-version backups.

Backup Exec Agent for Microsoft SharePoint

PROS: Performs well in basic backup and recovery of items in list and document libraries; includes the agent to back up the SQL Server databases; leverages existing Backup Exec infrastructure

CONS: Requires the basic Backup Exec server product

RATING: ◆◆◆◆◇

PRICE: $1,095.99 for a single-server environment

RECOMMENDATION: This product is a logical choice for a shop that already has a Backup Exec system. If you need more than backup and restore, look at the other products reviewed in this article.

CONTACT: Symantec • 800-754-6054 • www.symantec.com

Backup Exec Agent also supports multiple versions of SQL Server. Thus if you start your SharePoint deployment as a pilot project using SQL Server Express, you can upgrade to SQL Server 2005 with no loss of agent support. Backup Exec Agent supports both disk-to-tape and disk-to-disk backups, which is important for organizations using NAS or iSCSI storage. Additionally, it has the advantage of extending an interface that's already familiar to administrators.

Making the Choice

All four products reviewed reflect their vendor's perception of what a SharePoint administrator needs. If you already have Backup Exec, you can't go wrong by purchasing Backup Exec Agent for Microsoft SharePoint. Recovery Manager for SharePoint could be the right choice for administrators who are new to SharePoint (or just overworked), and it has a great price point. Replicator provides a unique method of disaster recovery that preserves the state of your SharePoint data, and DocAve is the total-control solution that large, dynamic SharePoint environments need. Although I was impressed with all the packages, DocAve 4.5 stands out as the most complete solution, and it's my pick for Editor's Choice.

InstantDoc ID 100126



Curt Spanburgh (cspanburgh@scg.net) is a contributing editor for *Windows IT Pro*, a Microsoft Dynamics CRM MVP, and a consultant for Solutions Consulting Group. He has worked with Microsoft applications for more than 20 years, and moderates the Microsoft Dynamics Support forum at www.minasi.com.



SharePoint Showcase

Your one-stop resource for SharePoint products and services

rackspace HOSTING

Rackspace Hosting offers flexible and customizable Sharepoint solutions backed by our Fanatical Support Promise™.

Let us manage your IT needs. We are here 24x7x365, Live.

www.rackspace.com/solutions/services/sharepoint.php

QUEST SOFTWARE®

Recovery Manager for SharePoint works with your existing backups so you can recover anything, anytime and restore it anywhere.

See for yourself – download a trial today!

www.quest.com/ShareTrial

SharePoint Virtual Event is Coming!

Microsoft Office SharePoint Server (MOSS) offers great functionality out of the box. But to get the most out of MOSS you need to think outside the box. This free one-day online conference will deliver the technical knowledge you need to kick MOSS up a notch.

Windows IT Pro

Register Today!

www.windowsitpro.com/go/sharepointvirtual

AvePoint®

DocAve v5 –The world's most powerful and award-winning solution for SharePoint backup, disaster recovery, administration, replication, archiving, compliance, and migration.

Unleash the power of SharePoint!

www.avepoint.com

SECURITY EXPLORER®

Move beyond the limitations of native tools and manage Sharepoint from Security Explorer's single interface, making your assessment, assignment and availability of Windows security easier.

www.scriptlogic.com/ad/witp/sxpsharepoint/092308

Free SharePoint Fundamentals CD

Learn how to uncover rich information management capabilities with this free SharePoint CD, written by independent, industry-leading SharePoint experts at *Windows IT Pro*.



Order Yours Today!

www.windowsitpro.com/go/cdfundamentals

Got SharePoint?

Then post your SharePoint solution here!

Build brand awarenss and preference with key SharePoint influencers in our SharePoint Showcase section.

Contact sales@windowsitpro.com or

800.621.1544

WinConnections

MICROSOFT EXCHANGE CONNECTIONS

UNIFIED COMMUNICATIONS CONNECTIONS

WINDOWS CONNECTIONS

SharePoint CONNECTIONS

MARCH 15-18, 2009

ORLANDO, FL • HYATT REGENCY GRAND CYPRESS

The cutting edge event for IT Professionals

Register by Jan 12th and receive a FREE night at JW Marriott.
(based on a 3-night minimum stay)



CHECK WEBSITE FOR DESCRIPTIONS OF SESSIONS AND WORKSHOPS

www.WinConnections.com

800.505.1201 • 203.268.3204







WinConnections

Where a passion for technology has no boundaries!

- 75+ MICROSOFT AND INDUSTRY EXPERTS
- 120+ IN-DEPTH SESSIONS
- UNPARALLELED WORKSHOPS
- EXCITING ANNOUNCEMENTS

New

- GREEN COMPUTING TRACK

Technology+Solutions+Impact

Connect to Microsoft and industry experts to separate technology myths from reality!



Steve Riley
Microsoft
Senior Security Strategist in Microsoft's Trustworthy Computing Group



Mark Minasi
MR&D
Best-selling Author, Popular Technology Columnist, Commentator



Dan Holme
Intelliem
Expert Consultant and Trainer

Microsoft® TechNet MAGAZINE TECH Conferences Inc. PENTON MEDIA Windows IT Pro SQL SERVER magazine

Enterprise Firewall Appliances

Burn up your security threats

by Jeff James

In a world filled with a menagerie of security threats—viruses, malware, phishing attempts, and outright hacking by cyber criminals—giving your IT infrastructure a solid security foundation is a must. An integral part of any network security strategy is the firewall appliance, an infrastructure component that can limit external access to your corporate network to only trusted users and organizations. Firewalls are available in both hardware and software varieties; in this buyer's guide I take a look at hardware firewall appliances priced at less than $15,000. Many advanced/deluxe firewall features are available by subscription only, so be sure to calculate the total cost of the firewall solution in addition to the cost of the base appliance.

Features Every Firewall Appliance Should Have

When you're shopping for a firewall appliance, you should start with the basics: Every product you examine should have an easy-to-use management console, provide basic perimeter defenses, accept TCP and UDP port blocking, support stateful inspection packet filtering, and be easily upgradable, both by swapping out existing hardware and replacing existing software. Beyond these basic features, here are some other things to watch for.

Throughput. According to Tony Howlett, CTO of the security consulting firm Network Security Services, matching a firewall appliance with your network throughput needs is essential. "Will [the firewall appliance] handle your network load in and out? Is it sized to provide room for growth in the future?" questions Howlett. "Or, will you have to replace the hardware if your [network-bandwidth needs] grow significantly?" According to a September 2007 report by the Gartner Group on enterprise network firewalls, the average maximum throughput of the firewall vendors they surveyed was 2.5Gbps of network traffic, and the intrusion prevention system (IPS) load of those same products averaged about 945Mbps. Getting a firewall appliance that can accommodate your data-throughput needs is just as important as acquiring other product features.

Manageability. The ability to manage your appliance effectively and centrally is a key to any product purchase, including enterprise firewalls. Many firewall vendors are particular about how they license their appliances. "In larger companies [with] certified experts on staff, an enterprise firewall from a large vendor often makes the most sense," says Howlett. "However, if you have a small IT staff with no specific expertise, you might want to consider one of the smaller [firewall appliance vendors] that use web interfaces and include some reporting software with their base units." Howlett adds that larger organizations also need to consider how easily they can manage a chosen product when using it with multiple units of the same appliance or with other firewall appliances from different vendors.

Extensibility. Many firewall appliance vendors have added extra security features to their products, making them much more than simple firewalls. "Appliances are using names such as 'unified threat management' and 'intrusion prevention system,'" says Howlett. "Some units let you add content filtering, email spam filtering, compliance monitoring, and more, all on the same box. However, if your network is large, having separate appliances might give you more flexibility in picking specific features and vendors." Many firewalls now provide VPN capabilities.

Don't Forget the Basics

Maintaining network security is one of the most important responsibilities of any IT professional, and it's vital that the products you choose have some important (albeit basic) features. "The ability to perform packet-, circuit-, and application-level filtering is especially important," says Windows IT Pro Technical Director Michael Otey. "This is especially important with the increasing use of web services and XML. The ability to perform caching is also another significant consideration."

Things to Avoid

In addition to looking for features your appliance *should* have, Howlett suggests that IT pros do their best to avoid making mistakes such as the following:

- Buying a firewall with an inadequate number of features or features that don't meet your needs. "You don't want to find out a few months or a year later that you have to upgrade," says Howlett.
- Buying a device that is too complicated or requires an inordinate amount of training and support costs.
- Buying into the "buzzword" mentality rather than investigating what the product actually does. Do you really need the very latest hardware with the catchy brand and feature names?
- Buying features you will never use.

"Make sure that you have the in-house or contract expertise to properly configure and maintain your firewall," says Howlett. "A badly configured firewall is nearly as bad as no firewall at all."

The world of network security is filled with cautionary tales

ENTERPRISE FIREWALL APPLIANCES

of enterprise firewall installations gone bad. Howlett has come across firewalls that haven't been updated or monitored for months (if not years), leaving critical vulnerabilities that the vendor patched and updated long ago. Some administrators never think to check their firewall vendor for firmware updates, a task that Howlett sees as vital. "You should treat [your firewall appliance] like any other OS, perhaps even more so because it guards the entrance to your network," says Howlett. "Be sure to regularly review [installed firewall appliances] for required updates and maintenance."

In the end, even the best product and

Vendor Information	Product	Pricing	Number of Switch Ports	Remote Clients? (y/n)	Site-to-Site Connections? (y/n)	Routable Network Interfaces? (y/n)	Stateful Packet Filtering? (y/n)	DHCP/DNS Services? (y/n)
Astaro 877-427-276 781-345-5000 www.astaro.com	Astaro Security Gateway	$345	Unrestricted	Y	Y	Y	Y	Y
Cisco Systems 800-553-6387 408-526-4000 www.cisco.com	Cisco ASA 5500 Series Adaptive Security Appliances	Begins at $595	Depends on model	Y	Y	Y	Y	Y
Fortinet 866-648-4638 408-235-7700 www.fortinet.com	FortiGate-310B	$6,995	10 firewall interfaces, 1 AMC slot	Y	Y	Y	Y	Y
Juniper Networks 866-298-6428 www.juniper.net	Juniper Networks Secure Services Gateway Series Product Family (SSG 5, SSG 20, SSG 140, SSG 320M, SSG 520M, SSG 550M)	$900 (SSG 5) to $10,500 (SSG 550M)	7 10/100 (SSG 5) to 44 10/100 (SSG 550M)	Y	Y	Y	Y	Y
NETASQ 33-320-619-630 44-1344-741003 www.netasq.com	F25, F50, F60, F200, F500	$985 (F25) to $12,460 (F500)	2 switch/5 ethernet (F25) to 4 switch + 2 GbE ports (F500)	Y	Y	Y	Y	Y
phion AG 43-508100 www.phion.com	phion M series	$7,700 (M3)	3x 10/100 (phion M) to 10x 10/100/1000 (Phion M5)	Y	Y	Y	Y	Y
Secure Computing 800-379-4944 408-494-2020 www.securecomputing.com	Secure Firewall (Sidewinder)	8 models from $1,900 to $69,900	4-24 (depends on model)	Y	Y	Y	N/A	Y
SonicWALL 888-557-6642 408-745-9600 www.sonicwall.com	SonicWALL E-Class NSA E6500, NSA E-5000, NSA 5000, NSA 4500, NSA 3500, NSA 2400	$13,995 (E6500) to $2,495 (NSA 2400)	6 to 8 (depends on model)	Y	Y	Y	Y	Y

a fault-free installation can't protect your network from human error or basic carelessness. "One customer had his Windows domain server open via RDP login attempts to the whole world with a simple administrator password," Howlett says. "It's a miracle it was never breached. Then again, maybe it *was* and the customer just never knew it."

InstantDoc ID 100185

JEFF JAMES (jjames@windowsitpro.com) is senior editor, products, for *Windows IT Pro* and *SQL Server Magazine*. He specializes in virtualization and terminal services and has over 15 years of experience as a writer and digital-content producer.

	Types of Alerts (list)	Logs Allowed Packets in Real Time? (y/n)	Logs Dropped Packets in Real Time? (y/n)	Report Output Formats (list)	Acts as Proxy? Forwards Packets? (y/n)	Content Filtering?	Diagnostic Tools?	Management Interface	ICSA Certification? (y/n)	Supports Failover Connections? (y/n)	DHCP-Aware VPN (y/n)	VPN-Aware DNS? (y/n)
	SNMP, email	Y	Y	HTML	Y/Y	Y	Y	HTTPS	Y	Y	Y	Y
	IPS alerts, SSL VPN alerts	Y	Y	Syslog, SNMP, SMTP, Netflow	Y/Y	Y (via content security module)	Y	CLI, ASDM	Y	Y	Y	Y
	Firewall, IPS, VPN	Y	Y	PDF, Word, text, MHT, HTML	Y/Y	Y	Y	HTTP, HTTPS, CLI	Y	Y	Y	Y
	Syslog, SNMP, email	Y	Y	PDF, HTML, RTF, XML, XLS	N/Y	Y	Y	HTTP, HTTPS, CLI (console, Telnet, SSH)	Y	Y	Y	Y
	SNMP, proprietary	Y	Y	HTML	Y / Y	Y	Y	GUI, CLI, SSH	Y	Y	N	Y
	Syslog, proprietary	Y	Y	PDF, HTML, XLS	Y/Y	Y	Y	CLI, GUI	N (CC EAL4+)	Y	Y	Y
	Email, pager	Y	Y	DEF, ASCII, binary, HTTP, XML, WebTrends	Y/Y	Y	Y	CLI, GUI	Y	Y	Y	Y
	Syslog, SNMP, local, SonicWALL Viewpoint	Y	Y	Syslog, email, SNMP	N/Y	Y	Y	HTTP, HTTPS, CLI, SSH	N (Pending)	Y	Y	Y

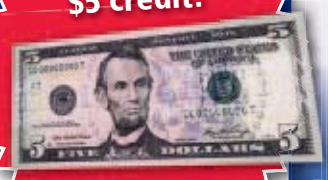
Making your holidays a little happier...

1&1 is including a **Holiday Bo**

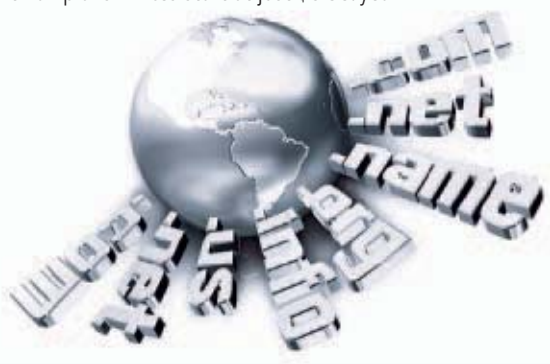


DOMAINS

Up to a $5 credit!*



Attract attention with a personalized domain! With 1&1's all-in-1 domain packages, you're not only getting a domain, but also a 5-page starter website builder and privacy protection. Private registration is included for FREE with all plans. Prices start at just $8.99/year.



WEB HOSTING

Up to a $50 credit!*



Get your website online today! Whether you're creating your first website, or you're a web professional, we offer web hosting packages for every skill level and budget. Our entry level packages start at just $3.99 per month.



Up to 5 FREE domains included!

*Credit amount dependent on package selected, and a minimum of between 12 months and 24 months contract term applies. Credit cannot be redeemed for cash. Visit www.1and1.com to view all applicable fees and full promotional offer details, terms and conditions. Product and program specifications, availability and prices subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet AG, all other trademarks are the property of their respective owners.

© 2008 1&1 Internet, Inc. All rights reserved

MEMBER OF united internet

call **1.877.go1and1**

nus with all web hosting plans!

As the world's largest web hosting provider, with more than 5 million hosted websites, we are committed to providing our customers with the progressive tools needed to develop and maintain an innovative web presence.

With 20 years of experience, 1&1 is dedicated to security, innovation and value when it comes to your website. As a 1&1 customer, you are not only assured your website is up and secure, but we also equip you with marketing and communication features to achieve success on the web.

Get a credit of up to $300 just for signing up!*



E-COMMERCE

Up to a $150 credit!*



Build your own eCommerce website! 1&1 eShops are a simplified eCommerce solution. Use the Setup Wizard to build your shop using customizable design templates, traffic boosting tools, and multiple payment options that suit your business and ensure your transactions are safe and secure. Prices start at $9.99 per month.



eBay compatible application

PayPal

SERVERS

Up to a $300 credit!*



NEW: 1&1 Premium Servers!
Our new servers with Quad-Core AMD Opteron™ Processors give you ultimate processing performance, cutting-edge, energy efficient technology and unparalleled reliability. Starting at $99.99 per month.

AMD Opteron™ 64



1&1

or visit us now **www.1and1.com**

■ Security ■ Messaging
■ Green Computing

INSIGHTS FROM THE INDUSTRY

Smart Card Reader Secures Multifunction Printers



One device that administrators haven't secured with a smart card is the lowly, yet hardworking, multifunction printer. Even for the admittedly smart card–savvy US Department of Defense (DoD), "imaging and printing are the biggest security holes," says Enrique Barkey, worldwide director, public sector at HP.

"The DoD realized a person could take a document and put it on a multifunction printer and send it by email straight out of an institution without any control," adds Simon Wakely, who is vice president of business development at smart card middleware provider ActivIdentity.

"It goes beyond the DoD. Even in commercial space, the weakest link is imaging and printing," says Barkey. "A lot of damage can be done because multifunction printers are connected to the network environment—they are the on and off ramp to the digital world."

As a result, HP teamed up with Activ Identity, creator of ActivClient smart card enablement software, to build a solution. The result: an HP multifunction printer that can read Common Access Card (CAC) smart cards and, via ActivIdentity middleware, communicate with Active Directory (AD) to authenticate employees to let them scan and email documents.

Here's how the printer authentication works. When the user sends a print job, it's encrypted, compressed, locked, and stored on a print server. Then, when the user goes to the printer to complete the print job (or to start a scan job), he or she must insert the CAC smart card into a reader at the multifunction printer. The printer prompts for a PIN, which the user enters. The middleware uses the PIN to unlock a secret area on the smart card; then, using public key infrastructure (PKI) to provide a certificate and AD to provide the information about the user, a credential is released and compared, and the response comes back: The user is approved.

> "Imaging and printing are the biggest security holes…even in the commercial space, the weakest link is imaging and printing. A lot of damage can be done [via a security breach] because multifunction printers are connected to the network environment."
>
> —Enrique Barkey, worldwide director, public sector at HP

Although the DoD requires authentication only for scanning documents, other organizations require authentication for printing documents—not only for security reasons but for cost-saving measures, especially in paper-intensive offices. "Printing costs can be a significant part of some organizations' budgets. A way to start controlling the printing environment is through security," says Barkey.

"ActivIdentity and HP have positioned this strong authentication solution into the private sector too," adds Wakely. "Smart cards are becoming ubiquitous as a strong form of authentication."

—Caroline Marwitz
InstantDoc ID 100280

Wanted: Your Real-World Experiences with Products

Have you discovered a great product that saves you time and money? Do you use something you wouldn't wish on anyone? Tell the world in a review right here in What's Hot: Readers Review Hot Products. If we publish your opinion, we'll send you a Best Buy gift card and a free VIP subscription to *Windows IT Pro*! Send information about a product you use and whether it helps you or hinders you to whatshot@windowsitpro.com.





Microsoft altiris LANDesk



KACE™

Deploy in days, not months.



No kidding around. Installing a KBOX by KACE gives you complete systems management in days, not months. We also do it for the lowest total cost of ownership. Give us a call, let us prove it.
Welcome to KACE Time.

EMA ALL-STAR 2008

Enterprise Management Associates
2008 Rising Star

KACE™
Systems Management. Done.

www.kace.com/deployindays 877.MGMT.DONE

KACE and KBOX are trademarks of KACE Networks Inc. All other registered trademarks are owned by their respective companies.

Green Consumers: Concern, but Not Much Action

Does the "greenness" of a product or service really make any difference to US consumers when they purchase a new PC or another product or service? A recent survey by The Diffusion Group (TDG) attempts to answer that and other questions concerning the relationship between consumers' perceptions and their behavior when it comes to green-related issues.

During second quarter 2008, TDG asked more than 1,500 US adult Internet users about their green-related activities, such as technology recycling habits (e.g., recycling of PC monitors, CPUs, inkjet cartridges); home-related green activities (e.g., installing energy-efficient appliances, adjusting thermostats to save energy); and travel-related green activities (e.g., driving below the speed limit, purchasing a hybrid automobile, carpooling). The survey also asked respondents to reveal their views on green issues, such as the relevancy of global warming and the environmental impact of their consumer electronics and technology purchases.

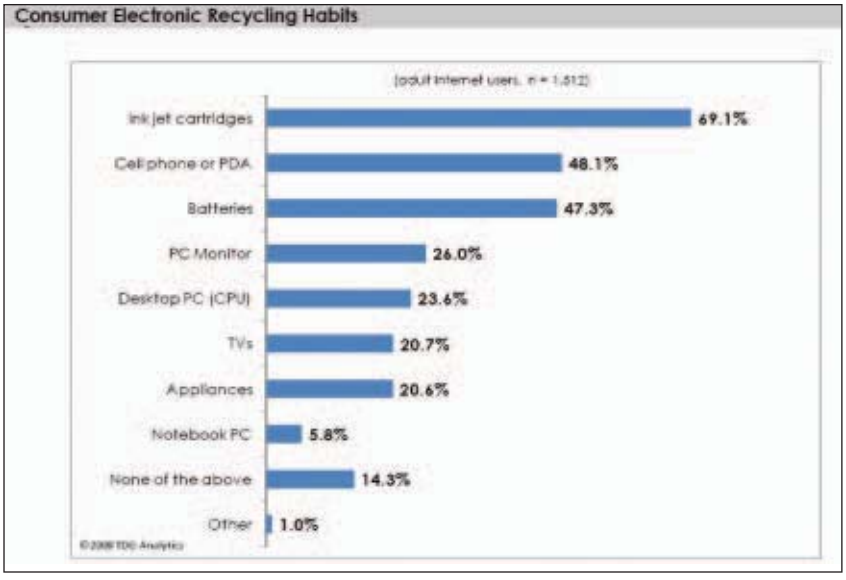
TDG released several key findings of the survey:

- More than half of adult consumers are concerned with the environmental impact from electronics they use. Ten percent express a critical concern, while 42 percent have no concern.
- The most tech-savvy consumers are not the optimal target for green technologies.
- Most consumers implement simple steps to reduce waste and protect the environment (e.g., recycling). However, only 5 percent of adult consumers engage in more intrusive steps (e.g., purchasing a hybrid vehicle, switching to an energy provider that uses alternative fuels).

TDG is publishing other key survey findings in two reports, both available for purchase. The first report gives an overview of what adult consumers perceive and how they behave regarding a variety of green-related issues. The second report will offer insight into how these perceptions translate into brand preferences and PC purchasing habits. To buy the reports, go to www.tdgresearch.com. (Only the first report, "It's Not Easy Being Green! Part 1: Eco-Friendly Attitudes & Behavior among U.S. Internet Consumers," was available at press time.)

For more information about green computing and purchasing behaviors, see "IT Decision Makers Reveal Their Views on Going Green," InstantDoc ID 99805, and "The Biggest Barriers to Going Green," InstantDoc ID 99926.

—Karen Bemowski
InstantDoc ID 99704



Groundbreaking Web Application Security!



NEW FROM THE PORT80 SECURITY SUITE:
ServerDefender VP protects your server from SQL Injection/XSS and more without signatures or setup hassles.

serverdefenderVP

Get PCI compliant today at:
port80software.com/security

30 DAY TRIALS

port80 software



PC Remote Control

Providing desktop support can be a headache with the large number of systems, servers and mobile devices located on today's corporate network. With NetSupport Manager remote control software, you can provide seamless IT support centrally from one location, improving response times and reducing associated IT costs.

Support, monitor and train your users securely over a LAN, WAN and the Internet. Manage and monitor multiple systems simultaneously with NSM's multi-platform support. Troubleshoot help requests efficiently with NSM's inventory and desktop management tools.

Able to co-exist with Remote Desktop (RDP), NetSupport Manager v10.3 supports a range of OS platforms and provides an option that lets any smart card login performed on a control PC to be redirected and applied on a client PC.

Take control of your network before it controls you.

NSM NETSUPPORT MANAGER

Mac Universal Windows solaris

770-205-4456
www.netsupportmanager.com

We've Found the Killer App . . . and It Is Voice

If your company is currently in the planning stages of a unified communications (UC) infrastructure, you need to consider the software you'll need to manage that environment, in addition to the hardware, networking, and telephony infrastructures and UC application software (e.g., email, IM). I recently spoke with two representatives of UC solution provider Clarus Systems—Brendan Reidy, president and CEO, and Gurmeet Lamba, senior vice president of product development—who shared their thoughts about the unique challenges UC brings to the enterprise and how UC management software can help IT meet those challenges.

According to Reidy, what makes UC tricky is that most people are coming from a legacy telephony world—a highly stable, closed environment. In that model, the average customer deals with his or her private branch exchange (PBX) only every two years to install updates. Today, with UC, we're looking at an IP world full of open architectures, and we're accessing that PBX nearly every day to install Wintel patches, security upgrades, and periodic vendor upgrades and establish new interfaces. It's a whole new mindset.

"The primary challenges to UC or even basic IP telephony," said Lamba, "are openness and drastic increases in complexity. However, the expectation from enterprise customers is still that a dial-tone is a God-given right. So the expectation is high reliability and high quality for the devices in the UC environment." Added Reidy, "The key component of UC is voice, so that has to be bulletproof."

I asked about how a good piece of UC management software should ideally tackle that all-important aspect of UC. "Well, I like to tell people, 'We've found the killer app—and it is 'voice,'" said Reidy. "Just look at how 'voice' has evolved! Historically, there was no doubt that networking was part of IT, and networking was just about data. So, we had all these sophisticated network-management tools—like IBM Tivoli, HP OpenView, Netcore, HP Network Node Manager—and the ability to do deep dives into network outages on the data network … and then there was telephony. I don't know of any company in which telephony reported to IT. It was never looked at strategically. Then we had the emergence of IP and VoIP, and people started saying 'Hey, my data network can also handle my voice traffic. I'm going to



share all these communications over the same pipe.' But the traditional tools on the market were completely inadequate to manage a voice network."

"Voice and UC should be just another app on your network," Lamba said. "In reality, it's intricate. It's a complex, large, interconnected set of apps that breaks easily unless you have the right management software. We're in the business of making voice and UC just another aspect of your network." One important aspect of a good UC management product is its ability to constantly ensure that communications are precise and available.

"In the investment banking world," Reidy said, "there's something called a Ready for Business check. At 6:00 A.M., the brokerage goes through a checklist—sort of like a jet at the airport before takeoff. They go through a checklist before saying, 'OK, we're ready for business today.' So, throughout the day, that brokerage's Ready for Business check is confirming that it's continually ready for business. Even this call we're on, there's a constant check to confirm that the call is satisfactory. It's taking the equivalent of a Mean Opinion Score (MOS)—developed in the early days of telephony—through several metrics every 8 seconds, looking for peaks and lows, and packet loss and jitter, then combining all those metrics into a database for the purpose of comparison, trending, and troubleshooting. Over the course of a day, we've caught things like loss of long-distance calling before end users even notice. We're constantly testing and monitoring networks."

"One of our approaches is automated testing," said Lamba. "We can have our product actually sitting in a data center and exercising all system functionality at night, making calls to a conference bridge, validating that everything is working correctly. After all, the best way to find problems is to actually try out the system. Everything we do takes an end-user perspective. If it's not working for the user at a certain level of satisfaction, the system isn't adequate. We literally see phones as network endpoints rather than just telephones."

"With ClarusIPC+, we focus on what we refer to as the four pillars of UC," Reidy said. "Those are testing, monitoring and management, configuration management, and business intelligence. In other words, how can I use the information gathered from my UC system and better run my business with that information?"

For more information about Clarus Systems' ClarusIPC+ product, which maximizes UC system availability and performance through automated, end-to-end testing, monitoring, reporting, troubleshooting, and operations management, go to www.clarussystems.com/products/clarusipc.php.

— Jason Bovberg

InstantDoc ID 100010







BI•lateral

bē-ī la-t(ə-)rəl
(adj.): of or relating to both the front and back ends of business intelligence

Windows IT Pro is your definitive source for BI tools.

LEARN from the top BI experts such as Derek Comingore and Dan Holme.

BUILD the best platforms and reports with help from *SQL Server Magazine*.

MASTER data-delivery with front-end solutions in *Windows IT Pro* magazine.

GET how-to information, industry trends, and commentary by experts with the new Essential BI UPDATE e-newsletter.

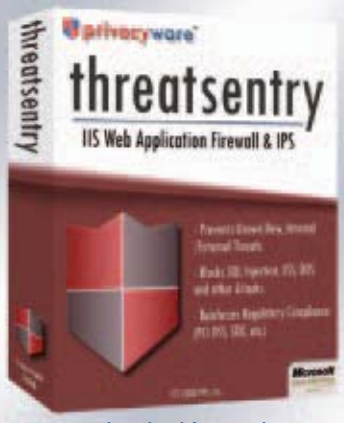
Choose the resource that's right for you.

www.windowsitpro.com/go/MyBI

Windows IT Pro | SQL Server Magazine

Are Your IIS Servers Under Attack?

Block all unwanted IIS traffic with ThreatSentry



download free trial

- IIS web application firewall & IPS
- stops known, new and internal threats
- blocks sql injection, xss, dos and more
- reinforces regulatory compliance

sales@privacyware.com • www.privacyware.com • 732.212.8110 x235

vizioncore™

Solutions For Every Stage of Your Virtualization Initiative

vConverter™
Physical to virtual (P2V), virtual to virtual (V2V) conversion to get you virtualized fast.

vAutomation Suite™
Heterogeneous administration, process automation and lifecycle management.

vRanger Pro™
Industry-leading backup and recovery solution for virtual servers.

vReplicator™
Replication to support high availability and disaster recovery.

vFoglight™
Monitoring for every level of the virtual infrastructure and at the application layer.

vOptimizer Pro™
Reclaim unused disk space to manage cost, storage and boost performance.

BEST OF vmworld 2008
NEW TECHNOLOGY FINALIST
vOptimizer Pro

Learn how Vizioncore's complete solution suite can help you achieve new levels of efficiency, flexibility and productivity. Register for the vSolutions webinar at www.vizioncore.com/vSolutions

www.vizioncore.com

Windows IT Pro Network

Search our network of sites dedicated to hands-on technical information for IT professionals.

www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.

www.windowsitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.

www.wininformant.com

EMAIL NEWSLETTERS

Get free NT/2000/XP/2003 news, commentary, and tips delivered automatically to your desktop.

- *Essential BI UPDATE*
- *Exchange & Outlook UPDATE*
- *.NET Briefing*
- *Scripting Central*
- *Security UPDATE*
- *SQL Server Magazine UPDATE*
- *Virtualization UPDATE*
- *Vista UPDATE*
- *Windows IT Pro UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Contact Joel Kirk at jkirk@penton.com.

Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.

www.windowsitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.

www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.

www.sqlmag.com

ASSOCIATED WEB SITES

WindowsDev Pro

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at WindowsDevPro.com, where IT pros creatively and proactively drive business value through technology.

www.windowsdevpro.com

Office & SharePoint Pro

Dive into Microsoft Office and SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.

www.officesharepointpro.com

For detailed information about products in this issue of *Windows IT Pro*, visit the Web sites listed below.

COMPANY/URL	PAGE
1&1 Internet www.1and1.com	62, 63
APC www.apc.com/promo	17
AvePoint Inc. www.avepoint.com	52, 57
Brocade Communications Systems www.brocade.com/fileintervention	Cover 4
Diskeeper Corporation www.diskeeper.com/tryitfree	50
GFI Software Ltd. www.gfi.com/wfl	21
HP www.hp.com/servers/rethink49	4
IBM Corporation www.ibm.com/green	43 ,45 ,47, 49
IBM Corporation www.ibm.com/systems/safedata	Cover 3
IT Watchdogs www.ITWatchDogs.com	69
Kace www.kace.com/deployindays	65
Lucid8 www.lucid8.com	11
Microsoft Corporation www.ServerUnleashed.com	30, 31
Microsoft Corporation www.microsoft.com/voip	Cover 2, 1
Microsoft Corporation www.SQLServerEnergy.com	7
Microsoft Corporation www.getonthecase.com	13
Microsoft Corporation www.microsoft.com/springboard	22, 23
Netikus www.eventsentry.com	24
Netsupport www.netsupportmanager.com	67
Port80 Software Inc. www.port80software.com/security	66
Privacyware www.privacyware.com	70
Quest Software Inc. www.quest.com/ShareTrial	57
Rackspace Managed Hosting www.rackspace.com/solutions/services/sharepoint	57
Sapien Technologies www.sapien.com	68
ScriptLogic Corporation www.scriptlogic.com/doitright	Cover tip
ScriptLogic Corporation www.scriptlogic.com/ad/witp/sxpharepoint/092308	57
St. Bernard Software www.stbernard.com/Anonymizer	40
Sunbelt Software Inc. www.sunbeltsoftware.com	8
Unisys www.unisys.com	32B
Vizioncore www.vizioncore.com/vSolutions	70
Windows Connections 2009 www.WinConnections.com	58
Windows IT Pro www.windowsitpro.com	14, 15, 57, 69, 70

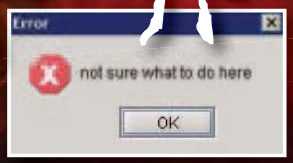
VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

ActivIdentity 64	Fortinet 60	phion AG 60
Astaro 60	HP 68	Prism Microsystems 48
BitDefender 48	Intel 38	Secure Computing Corporation 60
Cisco Systems 60	iStor Networks 48	SonicWALL, Inc 60
Citrix 48	Juniper Networks 60	Symantec 38
Clarus Systems 68	Mozilla 12	The Diffusion Group 66
eXpresso 48	NETASQ 60	

by Jason Bovberg

This Month's Signs of the Approaching Apocalypse



A dazzled computer



The invisibility cloak in action!

Air Force Develops Dazzling Laser Weapon

http://www.msnbc.msn.com/id/10268690

The Air Force recently developed a handheld laser weapon called "PHaSER" (for "Personal Halting and Stimulation Response") for use on the battlefield or on the streets of major cities. The weapon uses a two-wavelength laser system to temporarily blind (or "dazzle") an attacker. I don't know about you, but I prefer to play *Halo 3* in the comfort of my own home.



Invisibility Cloak on the Horizon, Scientists Say

http://news.cnet.com/8301-11386_3-10013127-76.html

Apparently, scientists might soon develop the ability to render people and objects invisible by redirecting light, like water flowing around a stone. It's all possible through the use of metamaterials, "artificially engineered structures created at a nano scale that contain optical properties not found in nature." Prominent proponents of this technology? High-school boys.

Our Top 10 Favorite Tech Quotes

10. "Technology is dominated by two types of people: those who understand what they do not manage, and those who manage what they do not understand." - Archibald Putt

9. "We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology."
- Carl Sagan



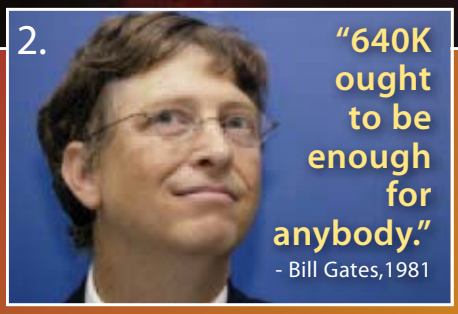
7. "I heard there's rumors on the Internets …".
- George W. Bush

6. "Never let a computer know you're in a hurry."- Anonymous

5. "Technology is like fish. The longer it stays on the shelf, the less desirable it becomes."- Andrew Heller, IBM

4. "Windows is just DOS in drag."
- Anonymous

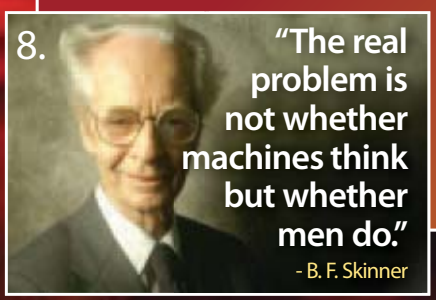
3. "If you tried to read every document on the web, then for each day's effort you would be a year further behind in your goal."
- Anonymous



2. "640K ought to be enough for anybody."
- Bill Gates,1981



1. "For years there has been a theory that millions of monkeys typing at random on millions of typewriters would reproduce the entire works of Shakespeare. The Internet has proven this theory to be untrue."
- Anonymous



8. "The real problem is not whether machines think but whether men do."
- B. F. Skinner

November 2008 issue no. 171, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Copyright 2008, Penton Media, Inc., all rights reserved. Subscriptions in US, $54.95 for one year; in Canada, $59 US currency, plus GST for one year; in all other countries, US $99. Windows is a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries, and *Windows IT Pro* is used under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation. Microsoft Corporation is not responsible in any way for the editorial policy or other contents of the publication. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 203-2782. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80539-0447. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 221 E. 29th St., Loveland, CO 80539. Printed in the USA. BPA Worldwide Member.

SEND US YOUR INDUSTRY HUMOR!

Email your industry humor, scandalous rumors, funny screenshots, favorite end-user moments, and IT-related pics to rumors@windowsitpro.com. If we use your submission, you'll receive a Ctrl+Alt+Del coffee mug.

GIVE YOUR DATA'S CONTINGENCY PLAN A CONTINGENCY PLAN.

intel Xeon® inside™
Powerful. Efficient.

IBM System x3350 Express

$905

OR $23/ MONTH FOR 36 MONTHS[1]

The more valuable your data, the more you need to protect it. Redundancy is critical. Like in the IBM System x3350™ Express. It comes with integrated RAID. Can our competitors say that? So if there's ever an unexpected problem on one drive, your business can keep running. Because the data you need is available in another location. Anytime you need it. Smart plan.

From the people and Business Partners of IBM.
It's innovation made easy.

HELP KEEP YOUR DATA SAFE AND ACCESSIBLE.



PN: 4192E1U

- Featuring Intel® Xeon® Processor (up to 3.0 GHz/6 MB/1333 MHz)
- Predictive Failure Analysis and Light Path Diagnostics, redundant, hot-swappable power supplies and fans and up to 4 hard disk drives
- Comes with a 1-year or 3-year customer replaceable unit and on-site limited warranty[2]

IBM SYSTEM x3650 EXPRESS

$5,409
OR $139/ MONTH FOR 36 MONTHS[1]



PN: 7979EVU

- Featuring up to two Intel® Xeon® Processors x5355
- Hot-swap redundant cooling, power and hard disk drives for high availability
- Comes with a 3-year on-site limited warranty[2] on parts and labor

IBM SYSTEM STORAGE DS3400 EXPRESS

$4,319
OR $111/ MONTH FOR 36 MONTHS[1]



PN: 172641E

- External Disk Storage with 1 Gbps Fibre Channel interface technology
- Built-in reliability features with dual-redundant power supplies standard

IBM EXPRESS "BUNDLE AND SAVE"

We bundle our Express systems to give you the accessories you need – while saving you money on the hardware you want. Act now. Available through **ibm.com** and IBM Business Partners.

IBM express advantage™

ibm.com/systems/safedata
1 866-872-3902 (mention 6N8AH09A)

1. IBM Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on an FMV lease of 36 monthly payments. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice. 2. IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, visit: ibm.com/servers/support/machine_warranties or write to: Warranty Information, P.O. Box 12195, RTP, NC 27709, Attn: Dept. JDJA/B203. IBM makes no representation or warranty regarding third-party products or services, including those designated as ServerProven® or ClusterProven®.Telephone support may be subject to additional charges. For on-site labor, IBM will attempt to diagnose and resolve the problem remotely before sending a technician. On-site warranty is available only for selected components. Optional same-day service response is available on [select] systems at an additional charge.

IBM, the IBM logo, IBM Express Advantage, System x and System Storage are trademarks of International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel and Xeon are registered trademarks of Intel Corporation. All other products may be trademarks or registered trademarks of their respective companies. All prices and savings estimates are based upon IBM's estimated retail selling prices as of 8/20/08. Prices and actual savings may vary according to configuration. Resellers set their own prices, so reseller prices and actual savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. IBM may not offer the products, features, or services discussed in this document in other countries. Prices are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or IBM Business Partner for the most current pricing in your geographic area. ©2008 IBM Corporation. All rights reserved.



FEEL LIKE YOU'RE STORING EVERYTHING AND MANAGING NOTHING? BROCADE FILES MANAGEMENT SOLUTIONS HELP YOU TAKE BACK CONTROL.
With Brocade Files Management Solutions, you can automatically and transparently migrate files to the optimum types of media based on your rules. So you can dramatically lower data management costs and gain more control of your file environment without compromising users' needs. And get a lot more breathing room. Get your FREE File Insight utility download at: www.brocade.com/fileintervention

BROCADE

© 2008 Brocade Communications Systems, Inc. All rights reserved. Brocade is a registered trademark, and the B-wing symbol is a trademark of Brocade Communications Systems, Inc.